Dell OpenManage Server Administrator Version 8.0.1

Benutzerhandbuch



Anmerkungen, Vorsichtshinweise und Warnungen



ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer besser einsetzen können.



VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.



WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2014 - 09

Rev. A00

Inhaltsverzeichnis

1 Einführung

Server Administrator bietet eine umfassende 1:1-Systemverwaltungslösung in zwei Formen: über eine integrierte Web-Browser-basierte grafische Benutzeroberfläche (GUI) und über eine Befehlszeilenschnittstelle (CLI) über das Betriebssystem. Server Administrator ermöglicht es Systemadministratoren, Systeme lokal und remote auf einem Netzwerk zu verwalten. Server Administrator ermöglicht es Systemadministratoren, sich auf die Verwaltung des gesamten Netzwerks zu konzentrieren. Dazu wird eine umfassende 1:1-Systemverwaltung zur Verfügung gestellt. Im Kontext von Server Administrators kann ein System ein Standalone-System, ein System mit verbundenen Netzwerkspeichereinheiten in einem separaten Gehäuse oder ein modulares System sein, das aus einem oder mehreren Servermodulen in einem modularen Gehäuse besteht. Server Administrator enthält Informationen über:

- Systeme, die korrekt funktionieren und Systeme mit Problemen
- Systeme, die Remote-Wiederherstellungsarbeiten erfordern

Server Administrator bietet benutzerfreundliche Verwaltung und Administration von lokalen Systemen und Remote-Systemen über eine umfassende Palette von integrierten Verwaltungsdiensten. Server Administrator ist die einzige Installation auf dem verwalteten System und ist sowohl lokal als auch im Remote-Zugriff über die Startseite von **Server Administrator** zugänglich. Auf Systeme, die im Remote-Zugriff überwacht werden, haben Sie über Einwähl-, LAN- oder Wireless-Verbindungen Zugang. Server Administrator gewährleistet die Sicherheit der Verwaltungsverbindungen durch rollenbasierte Zugriffssteuerung (RBAC), Authentifizierung sowie SSL-Verschlüsselung (Secure Socket Layer).

Installation

Sie können Server Administrator unter Verwendung der *DVD Dell Systems Management Tools and Documentation* installieren. Die DVD enthält ein Setup-Programm zum Installieren, Erweitern und Deinstallieren der Softwarekomponenten von Server Administrator, Managed System und Management Station. Zusätzlich können Sie Server Administrator mittels einer unbeaufsichtigten Installation über ein Netzwerk auf mehreren Systemen installieren. Das Server Administrator Installationsprogramm stellt Installationsskripts und RPM-Pakete bereit, um Server Administrator und andere Komponenten der Managed System Software auf dem verwalteten System zu installieren oder zu deinstallieren. Lesen Sie für weitere Informationen das *Server Administrator Installation Guide* (Server Administrator-Installationshandbuch) und das *Management Station Software Installation Guide* (Management Station Software-Installationshandbuch) unter **dell.com/opemanagemanuals**.



ANMERKUNG: Wenn Sie die OpenSource-Pakete von der *Dell Systems Management Tools and Documentation*-DVD installieren, werden die entsprechenden Lizenzdateien automatisch auf das System kopiert. Wenn Sie diese Pakete entfernen, werden auch die entsprechenden Lizenz-Dateien entfernt.

 ANMERKUNG: Bei einem modularen System muss Server Administrator auf jedem Servermodul im Gehäuse installiert werden.

Aktualisieren individueller Systemkomponenten

Um individuelle Systemkomponenten zu aktualisieren, verwenden Sie komponentenspezifische Dell Aktualisierungspakete. Verwenden Sie die DVD *Dell Server Update-Dienstprogramm*, um den vollständigen Versionsbericht anzuzeigen und ein gesamtes System zu aktualisieren. Server Update Utility (SUU) identifiziert die erforderlichen Aktualisierungen und wendet sie auf Ihr System an. SUU kann auch von **dell.com/support** heruntergeladen werden.

 ANMERKUNG: Weitere Informationen zur Beschaffung und Verwendung des Server-Aktualisierungsdienstprogramms (SUU), um Dell-Systeme zu aktualisieren oder die Aktualisierungen einzusehen, die für alle im Repository aufgelisteten Systeme verfügbar sind, finden Sie im *Dell Server Update Utility User's Guide* (Benutzerhandbuch für Dell Server-Update-Dienstprogramm) unter **dell.com/openmanagemanuals**.

Storage Management-Dienst

Der Storage Management-Dienst enthält Speicherverwaltungsinformationen in einer integrierten Graphikansicht.

 ANMERKUNG: Weitere Informationen zum Storage Management-Dienst finden Sie im Benutzerhandbuch zu *Server Administrator Storage Management User's Guide* (Benutzerhandbuch Server Administrator-Speicherverwaltung) unter **dell.com/openmanagemanuals**.

Instrumentationsdienst

Der Instrumentationsdienst gewährt schnellen Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von industriestandardmäßigen Systemverwaltungsagenten gesammelt werden, und erlaubt die Remote-Verwaltung überwachter Systeme, einschließlich Herunter- und Hochfahren des Systems und Sicherheit.

Remote-Access-Controller

Der Remote Access Controller stellt eine vollständige Remote System Management-Lösung für Systeme dar, die mit der DRAC-Lösung (Dell Remote Access Controller) oder der BMC/iDRAC-Lösung (Baseboard-Verwaltungs-Controller/Integrierter Dell Remote Access Controller) ausgestattet sind. Der Remote Access Controller gestattet externen Zugriff auf ein nicht funktionierendes System, wodurch es schnellstmöglich wieder in einen funktionierenden Zustand versetzt werden kann. Der Remote Access Controller bietet darüber hinaus eine Warnungsbenachrichtigung, wenn ein System ausgefallen ist, und ermöglicht den Neustart eines Systems im Remote-Zugriff. Darüber hinaus protokolliert der Remote Access Controller die wahrscheinliche Ursache von Systemabstürzen und speichert den letzten Bildschirm vor dem Absturz.

Protokolle

Server Administrator zeigt Protokolle von Befehlen, die das System erhalten oder selbst erzeugt hat, überwachte Hardwareereignisse und Systemwarnungen an. Sie können Protokolle auf der Startseite anzeigen lassen, diese ausdrucken oder als Bericht speichern und als E-Mail an einen von Ihnen festgelegten Service-Kontakt senden.

Was ist neu in dieser Version?

 ANMERKUNG: Server Administrator Version 8.0.1 wird nur auf den folgenden Systemen unterstützt:

- Dell PowerEdge R730
- PowerEdge R730 XD
- PowerEdge R630
- PowerEdge T630
- Dell Precision R7910

Folgendes sind die Highlights von Server Administrator Version 8.0.1:

- Unterstützung der folgenden Betriebssysteme:
  - Red Hat Enterprise Linux 7.0
  - VMware ESXi 5.5 U2 und 5.1 U2
  - Citrix XenServer 6.2 SP1
- Unterstützung für zusätzliche Attribute und Werte in BIOS-Setup-Gruppen. Weitere Informationen finden Sie unter *Command Line Interface Guide* (Befehlszeilenoberflächenhandbuch) unter **dell.com/openmanagemanuals**.
- Unterstützung der folgenden Netzwerkadapter:
  - Broadcom 5720 1-Gbit-bNDC
  - Intel 1350-Gbit-bNDC
  - Intel rNDC 10-Gbit-X710
  - Emulex OCm14104-UX-D 10-Gbit-rNDC
  - Emulex OCm14102-U2-D 10-Gbit-bNDC
  - Emulex OCm14102-U3-D 10-Gbit-Mezz
  - Emulex OCe14102-UX-D 10-Gbit-PCIe
- Unterstützung für Folgendes:
  - Dell PowerVault MD1400 und MD1420-Speichergehäuse
  - Dell PowerEdge S130 Software-RAID-Lösung
  - Dell PowerEdge RAID-Controller 9-Karten - H730, H730P, H830 und H330
  - 12-GBit/s-SAS-HBA-Controller

– Controller-Modus-Auflistung (RAID und HBA)

- Veraltete Unterstützung für SNMP-Set-Funktion.

Verfügbarkeit von Systemverwaltungsstandards

Server Administrator unterstützt die folgenden Systemverwaltungsprotokolle:

- HTTPS (HyperText Transfer Protocol Secure)
- CIM (Common Information Model, gemeinsames Informationsmodell)
- Simple Network Management Protocol (SNMP)

Wenn Ihr System SNMP unterstützt, müssen Sie den Dienst auf Ihrem Betriebssystem installieren und aktivieren. Wenn SNMP-Dienste auf Ihrem Betriebssystem verfügbar sind, installiert das Server Administrator-Installationsprogramm die unterstützenden Agenten für SNMP.

HTTPS wird auf allen Betriebssystemen unterstützt. Die Unterstützung für CIM und SNMP ist betriebssystemabhängig und in einigen Fällen auch von der Version des Betriebssystems abhängig.



ANMERKUNG: Informationen zu SNMP-Sicherheitsbedenken finden Sie in der Infodatei zu Server Administrator (im Lieferumfang der Server Administrator-Anwendung enthalten) oder unter **dell.com/openmanagemanuals**. Sie müssen Aktualisierungen von den Master-SNMP-Agenten Ihres Betriebssystems anwenden, um sicherzustellen, dass die SNMP-Subagenten von Dell sicher sind.

Verfügbarkeit auf unterstützten Betriebssystemen

Auf unterstützten Microsoft Windows-Betriebssystemen unterstützt Server Administrator zwei Systemverwaltungsstandards: CIM/WMI (Windows Management Instrumentation) und SNMP, während Server Administrator auf unterstützten Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssystemen den SNMP-Systemverwaltungsstandard unterstützt.

Server Administrator fügt bedeutende Sicherheit zu Systemverwaltungsstandards hinzu. Alle Attributeinstellungsvorgänge (z. B. Ändern des Werts einer Systemkennnummer) müssen mit Dell OpenManage Essentials ausgeführt werden, während eine Anmeldung mit der erforderlichen Berechtigung besteht.

Die folgende Tabelle zeigt die Verfügbarkeit der Systemverwaltungsstandards für jedes unterstützte Betriebssystem.

Tabelle 1. Verfügbarkeit von Systemverwaltungsstandards

Betriebssystem	SNMP	CIM
Microsoft Windows Server 2008-Reihe	Auf dem Installationsmedium des Betriebssystems verfügbar	Immer installiert
Red Hat Enterprise Linux	Verfügbar im net-snmp-Paket auf dem Betriebssystem-Installationsdatenträger	Nicht verfügbar
SUSE Linux Enterprise Server	Verfügbar im net-snmp-Paket auf dem Betriebssystem-Installationsdatenträger	Nicht verfügbar
VMware ESXi	SNMP-Trap-Support verfügbar	Verfügbar

Betriebssystem	SNMP	CIM
	ANMERKUNG: ESXi unterstützt SNMP-Traps, nicht jedoch Hardwarebestandsaufnahme über SNMP.	
Citrix XenServer 6.0	Verfügbar im net-snmp-Paket auf dem Betriebssystem-Installationsdatenträger	Nicht verfügbar

Server Administrator-Startseite

Die Startseite von **Server Administrator** bietet einfach einrichtbare und leicht anwendbare Web-Browser-basierte Systemverwaltungsaufgaben über das verwaltete System oder über einen Remote-Host über ein LAN, einen DFÜ-Dienst oder ein drahtloses Netzwerk. Wenn der Dell Systems Management Server Administrator-Verbindungsdienst (DSM SA-Verbindungsdienst) installiert ist und auf dem verwalteten System konfiguriert wird, können Sie Remote-Verwaltungsfunktionen von jedem System ausführen, das einen unterstützten WWW-Browser und Verbindung hat. Zusätzlich enthält die Startseite von Server Administrator eine ausführliche, kontextabhängige Online-Hilfe.

Weitere nützliche Dokumente

Zusätzlich zu dieser Anleitung können Sie auf die folgenden Anleitungen zugreifen, die unter **dell.com/softwaresecuritymanuals** zur Verfügung stehen.

- *Die Dell Systems Software Support Matrix* (Dell Systems Software Support-Matrix) bietet Informationen über die verschiedenen Dell-Systeme, die durch diese Systeme unterstützten Betriebssysteme und die Komponenten, die auf diesen Systemen installiert werden können.
- Das *Server Administrator Installation Guide* (Installationshandbuch zu Dell OpenManage Server Administrator) enthält Anleitungen zur Installation von Dell OpenManage Server Administrator.
- Das *Management Station Software Installation Guide* (Dell OpenManage Management Station Software-Installationshandbuch) enthält Anweisungen für die Installation der Dell OpenManage Management Station-Software.
- Das *OpenManage SNMP Reference Guide* (OpenManage SNMP-Referenzhandbuch) enthält die SNMP-Verwaltungsinformationen-Datenbank (MIB).
- Das *Dell OpenManage Server Administrator CIM Reference Guide* (Dell OpenManage Server Administrator-CIM-Referenz-Handbuch) dokumentiert den Anbieter des Allgemeinen Informationsmodells (CIM), eine Erweiterung der standardmäßigen MOF-Datei (Management Object Format).
- Im *Messages Reference Guide* (Meldungs-Referenzhandbuch) sind die Meldungen aufgeführt, die im Warnungsprotokoll auf der Startseite von Server Administrator oder auf der Ereignisanzeige des Betriebssystems angezeigt werden.
- Das *Server Administrator Command Line Interface Guide* (Benutzerhandbuch für die Server Administrator-Befehlszeilenschnittstelle) dokumentiert die vollständige Befehlszeilenschnittstelle für Server Administrator.
- Das *Dell Chassis Management Controller User's Guide* (Dell Chassis Management Controller-Benutzerhandbuch) enthält umfassende Informationen über die Verwendung des Controllers, der alle Module im Gehäuse, das das Dell-System enthält, verwaltet.
- Das *Dell Online Diagnostics User's Guide* (Dell Online Diagnostics-Benutzerhandbuch) bietet umfassende Informationen über die Installation und Verwendung von Onlinediagnose auf Ihrem System.

- Das *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Dell OpenManage Baseboard Management Controller Utilities-Handbuch) enthält zusätzliche Informationen über die Verwendung des Server Administrators zur Konfiguration und Verwaltung des System-BMC.
- Das *Dell OpenManage Server Administrator Storage Management User's Guide* (Dell OpenManage Server Administrator Storage Management-Benutzerhandbuch) ist ein umfassendes Nachschlagewerk für die Konfiguration und Verwaltung lokaler und externer Speicherkomponenten, die an ein System angeschlossen sind.
- Im *Dell Remote Access Controller Racadm User's Guide* (Benutzerhandbuch zum Dell Remote Access Controller / Racadm) finden Sie Informationen zur Verwendung des racadm-Befehlszeilen-Dienstprogramms.
- Das *Dell Update Packages User's Guide* (Benutzerhandbuch zu den Dell Update Packages) enthält Informationen über das Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Das *Dell OpenManage Server Update Utility User's Guide* (Dell OpenManage Server Update Utility-Benutzerhandbuch) bietet Informationen über Beschaffung und Verwendung des Server-Aktualisierungsdienstprogramms (SUU), um Dell-Systeme zu aktualisieren oder die Aktualisierungen einzusehen, die für alle im Repository aufgelisteten Systeme verfügbar sind.
- Das *Dell Management Console User’s Guide* (Benutzerhandbuch der Dell Management Console) enthält Informationen zur Installation, Konfiguration und Verwendung der Dell Management Console.
- Das *Dell Lifecycle Controller User Guide* (Benutzerhandbuch zum Dell Life Cycle Controller) enthält Informationen zum Einrichten und Verwenden des Unified Server Configurator, um System- und Speicherverwaltungs-Tasks über die gesamte Lebensdauer des Systems durchführen zu können.
- Das *Glossar* mit Informationen zu den in diesem Dokument verwendeten Begriffen.

Zugriff auf Dokumente der Dell Support-Website

Sie können auf eine der folgenden Arten auf die folgenden Dokumente zugreifen:

- Verwendung der folgenden Links:
  - Für alle Enerprise Systems Management-Dokumente – **dell.com/softwaresecuritymanuals**
  - Für Enterprise Systems Management-Dokumente – **dell.com/openmanagemanuals**
  - Für Remote Enterprise Systems Management-Dokumente – **dell.com/esmmanuals**
  - Für OpenManage Connections Enterprise Systems Management-Dokumente – **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Für Tools für die Betriebsfähigkeitsdokumente – **dell.com/serviceabilitytools**
  - Für Client Systems Management-Dokumente – **dell.com/clientsystemsmanagement**
  - Für OpenManage Connections Client Systems Management-Dokumente – **dell.com/connectionsclientsystemsmanagement**
- Gehen Sie auf der Dell Support-Website folgendermaßen vor:
  a. Rufen Sie die Website **dell.com/support/home** auf.
  b. Klicken Sie unter **Allgemeiner Support** auf **Software & Sicherheit**.
  c. Klicken Sie im Gruppenfeld **Software & Sicherheit** auf einen der folgenden Links:
     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Tools für die Betriebsfähigkeit**
     - **Client Systems Management**

- **Connections Client Systems Management**

d. Um ein Dokument anzuzeigen, klicken Sie auf die jeweilige Produktversion.

- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen" ein.

Wie Sie technische Unterstützung erhalten

Wenn Sie ein in diesem Handbuch beschriebenes Verfahren nicht verstehen, oder wenn Ihr Produkt nicht die erwartete Leistung erbringt, stehen Ihnen zur Unterstützung Hilfsprogramme zur Verfügung. Weitere Informationen über diese Hilfsprogramme finden Sie unter **Wie Sie Hilfe bekommen** im *Hardware-Benutzerhandbuch* des Systems.

Ferner bietet Dell Unternehmensschulungen und Zertifizierungen an; weitere Informationen finden Sie unter dell.com/training. Dieser Service wird unter Umständen nicht an allen Standorten verfügbar sein.

Kontaktaufnahme mit Dell



ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

Besuchen Sie die Website **dell.com/contactdell.**

2

Setup und Administration

Der Server Administrator bietet Sicherheit durch rollenbasierte Zugriffsregelung (RBAC), Authentisierung und Verschlüsselung für die Internet-basierte und die Befehlszeilen-Schnittstelle.

Rollenbasierte Zugangskontrolle

RBAC erreicht Sicherheit durch Festlegung der Vorgänge, die von Personen in besonderen Funktionen ausgeführt werden können. Jedem Benutzer werden eine oder mehrere Rollen zugeteilt und jeder Rolle sind eine oder mehrere Berechtigungen zugewiesen, die für die Benutzer in dieser Rolle zugelassen sind. Mit RBAC entspricht Sicherheitsverwaltung genau der Organisationsstruktur.

Benutzerberechtigungen

Server Administrator gewährt unterschiedliche Zugriffsrechte basierend auf den dem Benutzer zugewiesenen Gruppenberechtigungen. Die vier Benutzerebenen lauten: Benutzer, Hauptbenutzer, Administrator und Administrator mit erhöhten Rechten.

Tabelle 2. Benutzerberechtigungen

Benutzerberechtigungsebene	Zugriffstyp		Beschreibung
	Ansicht	**Verwalten**	
Benutzer	Ja	Nein	*Benutzer* können die meisten Informationen anzeigen.
Hauptbenutzer	Ja	Ja	*Hauptbenutzer* können Warnungsschwellenwerte einstellen und konfigurieren, welche Warnungsmaßnahmen ausgeführt werden sollen, wenn ein Warnungs- oder Fehlerereignis eintritt.
Administrator	Ja	Ja	*Administratoren* können Maßnahmen zum Herunterfahren konfigurieren und durchführen, automatische Wiederherstellungsmaßnahmen für den Fall konfigurieren, dass ein Betriebssystem auf einem System nicht mehr reagiert, und Hardware-, Ereignis- und Befehlsprotokolle löschen. Administratoren können das System auch konfigurieren, um E-Mails zu senden.
Administrator mit erhöhten Rechten (nur Linux)	Ja	Ja	*Administratoren mit erhöhten Rechten* können Informationen anzeigen und verwalten.

Berechtigungsebenen für den Zugriff auf Server Administrator-Dienste

Die folgenden Tabelle werden die Benutzer zusammengefasst, die Berechtigungen für den Zugriff auf Server Administrator-Dienste und deren Verwaltung aufweisen.

Der Server Administrator erteilt Benutzern, die mit *Benutzer*berechtigungen angemeldet sind, Nur-Lese-Zugriff. Benutzer mit *Hauptbenutzer*berechtigungen erhalten Lese- und Schreibzugriff, während Benutzer, die mit Administratorrechten oder erhöhten Administratorrechten angemeldet sind, Lese-, Schreib- und Administrator-Zugriffsrechte erhalten.

Tabelle 3. Benutzerberechtigungen für die Verwaltung von Server Administrator-Diensten

Dienstleistung	Erforderliche Benutzerberechtigungsebene	
	Ansicht	**Verwalten**
Instrumentation	Benutzer, Hauptbenutzer, Administrator, Administrator mit erhöhten Rechten.	Hauptbenutzer, Administrator, Administrator mit erhöhten Rechten.
Remote-Zugriff	Benutzer, Hauptbenutzer, Administrator, Administrator mit erhöhten Rechten.	Administrator, Administrator mit erhöhten Rechten.
Speicherverwaltung	Benutzer, Hauptbenutzer, Administrator, Administrator mit erhöhten Rechten.	Administrator, Administrator mit erhöhten Rechten.

Authentifizierung

Das Server Administrator-Authentisierungsschema stellt sicher, dass die richtigen Zugriffstypen den korrekten Benutzerberechtigungen zugewiesen werden. Darüber hinaus validiert das Server Administrator-Authentifizierungsschema den Kontext, in dem das gegenwärtige Verfahren ausgeführt wird, wenn die Befehlszeilenschnittstelle (CLI) aufgerufen wird. Dieses Authentifizierungsschema stellt sicher, dass alle Server Administrator-Funktionen korrekt authentifiziert werden, wobei es keine Rolle spielt, ob über die Startseite von Server Administrator oder über die CLI auf sie zugegriffen wird.

Microsoft Windows-Authentifizierung

Für unterstützte Microsoft Windows-Betriebssysteme verwendet die Server Administrator-Authentifizierung Integrated Windows Authentication (früher als NTLM bekannt), um zu authentifizieren. Dieses Authentifizierungssystem ermöglicht den Einbezug der Server Administrator-Sicherheit in ein Gesamtsicherheitsschema für das Netzwerk.

Red Hat® Enterprise Linux- und SUSE® Linux Enterprise Server-Authentifizierung

Für unterstützte Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssysteme verwendet Server Administrator verschiedene Authentifizierungsmethoden, die auf der PAM-Bibliothek basieren (Pluggable Authentication Modules). Benutzer können sich entweder lokal oder im Remote-Zugriff bei Server Administrator anmelden und verschiedene Kontoverwaltungsprotokolle, wie z. B. LDAP, NIS, Kerberos und Winbind verwenden.

VMware ESXi Server 5.X-Authentifizierung

ESXi Server authentifiziert Benutzer, die auf ESXi-Hosts zugreifen, unter Verwendung des vSphere/VI Client oder Software Development Kit (SDK). Für die Standardinstallation von ESXi wird eine lokale Kennwortdatenbank für die Authentifizierung verwendet. ESXi-Authentifizierungstransaktionen mit Server Administrator sind auch direkte Interaktionen mit dem **vmware-hostd**-Ablauf. Um sicherzustellen, dass die Authentifizierung für Ihre Website wirksam funktioniert, führen Sie grundlegende Tasks wie die folgenden durch: Einrichten von Benutzern, Gruppen, Berechtigungen und Rollen, Konfigurieren von Benutzerattributen, Hinzufügen Ihrer eigenen Zertifikate und Bestimmen, ob SSL verwendet werden soll.



ANMERKUNG: Auf Systemen, auf denen das VMware ESXi Server 5.0 -Betriebssystem ausgeführt wird, benötigen sämtliche Benutzer-Administratorrechte, um sich bei Server Administrator anmelden zu können. Informationen zur Rollenzuweisung finden Sie in der VMware-Dokumentation.

Verschlüsselung

Zugriff auf den Server Administrator erfolgt über eine sichere HTTPS-Verbindung mittels Secure Socket Layer-Technologie (SSL) zur Gewährleistung und zum Schutz der Identität des verwalteten Systems. Java Secure Socket Extension (JSSE) wird von unterstützten Microsoft Windows-, Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssystemen zum Schutz der Benutzeranmeldeinformationen und anderer sensibler Daten verwendet, die über die Socket-Verbindung übertragen werden, wenn ein Benutzer auf die Startseite von **Server Administrators** zugreift.

Benutzerberechtigungen zuweisen

Allen Benutzern der Dell OpenManage-Software müssen Benutzerberechtigungen zugewiesen werden, bevor die Dell OpenManage-Software installiert wird, um die Sicherheit kritischer Systemkomponenten zu gewährleisten. Neue Benutzer können sich bei der Dell OpenManage-Software mit ihren Benutzerberechtigungen anmelden.



VORSICHT: Weisen Sie jedem Benutzerkonto, das auf Dell OpenManage Software zugreifen kann, ein Kennwort zu, um Ihre kritischen Systemkomponenten vor Zugriff zu schützen.



VORSICHT: Gastkonten sollten für unterstützte Windows-Betriebssysteme deaktiviert sein, um Ihre kritischen Systemkomponenten vor Zugriff zu schützen. Nennen Sie möglicherweise die Gastkonten um, um zu verhindern, dass die Remote-Skripte die Konten über die Standard-Gastkontonamen aktivieren können.



ANMERKUNG: Bei Fragen zur Zuweisung von Benutzergruppenberechtigungen für jedes unterstützte Betriebssystem lesen Sie die Dokumentation zum Betriebssystem.



ANMERKUNG: Wenn Sie Benutzer zur OpenManage-Software hinzufügen wollen, fügen Sie dem Betriebssystem neue Benutzer hinzu. Sie müssen keine neuen Benutzer in der OpenManage-Software erstellen.

Benutzer einer Domäne auf Windows-Betriebssystemen hinzufügen

 ANMERKUNG: Für die Durchführung der folgenden Verfahren muss Microsoft Active Directory auf dem System installiert sein. Weitere Informationen zur Verwendung des Active Directory finden Sie im Abschnitt Active Directory-Anmeldung verwenden.

1. Wechseln Sie zu **Systemsteuerung** → **Verwaltung** → **Active Directory-Benutzer und Computer**.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Benutzer**, oder klicken Sie mit der rechten Maustaste auf den Container, dem Sie den neuen Benutzer hinzufügen möchten, und gehen Sie dann zu **Neuer** → **Benutzer**.
3. Geben Sie die entsprechenden Benutzernameninformationen in das Dialogfeld ein und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.
5. Doppelklicken Sie auf das Symbol für den eben erstellten Benutzer.
6. Klicken Sie auf das Register **Mitglied von**.
7. Klicken Sie auf **Add** (Hinzufügen).
8. Wählen Sie die entsprechende Gruppe und klicken Sie auf **Hinzufügen**.
9. Klicken Sie zweimal hintereinander auf **OK.**

    ANMERKUNG: Neue Benutzer können sich bei der Dell OpenManage-Software mit den Benutzerberechtigungen der ihnen zugewiesenen Gruppe oder Domäne anmelden.

Server Administrator-Benutzer für unterstützte Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssysteme erstellen

Die Administratorberechtigungen werden dem als root angemeldeten Benutzer zugewiesen. Weitere Informationen über das Erstellen von Benutzern und Benutzergruppen erhalten Sie in der Dokumentation zum Betriebssystem.

 ANMERKUNG: Sie müssen als `root` oder gleichwertiger Benutzer angemeldet sein, um die folgenden Verfahren auszuführen.

 ANMERKUNG: Für die Durchführung dieser Verfahren muss das Dienstprogramm **useradd** auf dem System installiert sein.

Zugehörige Links:

- Benutzer mit Benutzerberechtigungen erstellen
- Benutzer mit Hauptbenutzerberechtigungen erstellen

Benutzer mit Benutzerberechtigungen erstellen

1. Führen Sie den folgenden Befehl von der Befehlszeile aus: `useradd -d <home-directory> -g <group> <username>` wobei `<group>` nicht `root` ist.

    ANMERKUNG: Wenn `<group>` nicht existiert, muss sie mit dem Befehl **groupadd** erstellt werden.
2. Geben Sie `passwd <username>` ein und drücken Sie <Eingabe>.
3. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den neuen Benutzer ein.

    ANMERKUNG: Weisen Sie jedem Benutzerkonto mit Zugriff auf den Server Administrator ein Kennwort zu, um den Zugriff auf die kritischen Systemkomponenten zu schützen.

Der neue Benutzer kann sich jetzt mit Benutzergruppen-Zugriffsrechten bei Server Administrator anmelden.

Benutzer mit Hauptbenutzerberechtigungen erstellen

1. Führen Sie den folgenden Befehl von der Befehlszeile aus: useradd -d <*home-directory*> -g <*gruppe*> <*Benutzername*>

   ANMERKUNG: Stellen Sie als primäre Gruppe root ein.

2. Geben Sie passwd <*Benutzername*> ein und drücken Sie <Eingabe>.
3. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den neuen Benutzer ein.

   ANMERKUNG: Weisen Sie jedem Benutzerkonto mit Zugriff auf den Server Administrator ein Kennwort zu, um den Zugriff auf die kritischen Systemkomponenten zu schützen.

   Der neue Benutzer kann sich jetzt mit Hauptbenutzergruppen-Zugriffsrechten bei Server Administrator anmelden.

Server Administrator-Benutzerberechtigungen bei Linux-Betriebssystemen bearbeiten

ANMERKUNG: Sie müssen als root oder gleichwertiger Benutzer angemeldet sein.

1. Öffnen Sie die Datei **omarolemap**, die sich unter /opt/dell/srvadmin/etc/omarolemap befindet.
2. Fügen Sie in der Datei Folgendes hinzu: <*Benutzername*>[Tab]<*Hostname*>[Tab]<*Rechte*>

   Die folgenden Tabelle listet die Legende für das Hinzufügen der Rollendefinition zu **omarolemap** auf.

   Tabelle 4. Legende für das Hinzufügen der Rollendefinition in Server Administrator

<Benutzername>	<Hostname>	<Rechte>
Benutzername	Host-Name	Administrator
(+)Gruppenname	Domäne	Benutzer
Platzhalter (*)	Platzhalter (*)	Benutzer
[Tab] = \t (tab character)		

   Die folgenden Tabelle listet die Beispiele für das Hinzufügen der Rollendefinition zur Datei **omarolemap** auf.

   Tabelle 5. Beispiele für das Hinzufügen der Rollendefinition in Server Administrator

<Benutzername>	<Hostname>	<Rechte>
Bob	Ahost	Hauptbenutzer
+root	Bhost	Administrator
+root	Chost	Administrator
Bob	*.aus.amer.com	Hauptbenutzer
Mike	192.168.2.3	Hauptbenutzer

3. Speichern und schließen Sie die Datei.

Bewährte Verfahren bei der Verwendung der omarolemap-Datei

Nachfolgend sind die bewährten Verfahren aufgeführt, die im Zusammenhang mit der **omarolemap**-Datei berücksichtigt werden sollten:

- Löschen Sie nicht die folgenden Standardeinträge in der **omarolemap**-Datei.

root	* Administrator
+root	* Hauptbenutzer
*	* Benutzer

- Ändern Sie nicht die **omarolemap**-Dateiberechtigungen oder das Dateiformat.
- Verwenden Sie die Loop Back-Adresse nicht für `<Hostname>`, z. B.: localhost oder 127.0.0.1.
- Wenn die Änderungen für die Datei **omarolemap** nach einem Neustart der Verbindungsdienste nicht wirksam werden, konsultieren Sie das Befehlsprotokoll, um die Fehler einzusehen.
- Wenn die **omarolemap**-Datei von einem System zu einem anderen kopiert wird, müssen die Dateiberechtigungen und Einträge der Datei erneut überprüft werden.
- Dem `Gruppennamen` muss ein + als Präfix vorangehen.
- Server Administrator verwendet in den folgenden Fällen die standardmäßigen Betriebssystembenutzerberechtigungen:
  - Ein Benutzer wird in der **omarolemap**-Datei heruntergestuft.
  - Es sind doppelte Einträge für Benutzernamen oder Gruppen mit dem gleichen `<Hostnamen>` vorhanden.
- `Space` können anstelle von `[Tab]` als Begrenzungszeichen für Spalten verwendet werden.

Server Administrator-Benutzer für VMware ESXi 5.X und ESXi 6.X erstellen

So fügen Sie der Tabelle "Benutzer" einen Benutzer hinzu:

1. Melden Sie sich unter Verwendung des vSphere Client beim Host an.
2. Klicken Sie auf das Register **Benutzer und Gruppen** und klicken Sie auf **Benutzer**.
3. Klicken Sie auf eine beliebige Stelle in der Tabelle "Benutzer" und klicken Sie auf **Hinzufügen**, um das Dialogfeld **Neuen Benutzer hinzufügen** zu öffnen.
4. Geben Sie einen Anmeldenamen, einen Benutzernamen, eine numerische Benutzer-ID (UID) sowie ein Kennwort ein; das Festlegen des Benutzernamens und die UID ist optional. Wenn Sie die UID nicht festlegen, weist der vSphere Client die nächste verfügbare UID zu.
5. Um einem Benutzer zu erlauben, über eine Befehls-Shell auf den ESXi-Host zuzugreifen, wählen Sie **Diesem Benutzer Shell-Zugriff gewähren** aus. Benutzer, die ausschließlich über den vSphere Client auf den Host zugreifen, benötigen keinen Shell-Zugriff.
6. Sie können den Benutzer zu einer Gruppe hinzufügen, indem Sie den Gruppennamen aus dem Drop-Down-Menü **Gruppe** auswählen und auf **Hinzufügen** klicken.
7. Klicken Sie auf **OK**.

Gastkonten und anonyme Konten in unterstützten Windows-Betriebssystemen deaktivieren



ANMERKUNG: Sie müssen mit Administrator-Berechtigungen angemeldet sein.

1. Öffnen Sie das Fenster **Computerverwaltung**.
2. Erweitern Sie in der Konsolenstruktur das Fenster **Lokale Benutzer und Gruppen** und klicken Sie auf **Benutzer**.

3. Doppelklicken Sie das Benutzerkonto **Gast** oder **IUSR_Systemname**, um die Eigenschaften für diese Benutzer anzuzeigen, oder klicken Sie mit der rechten Maustaste auf das Benutzerkonto **Gast** oder **IUSR_***Systemname* und wählen Sie **Eigenschaften** aus.
4. Wählen Sie **Konto ist deaktiviert** und klicken Sie auf **OK**.

   Es wird ein roter Kreis mit einem X über dem Benutzernamen angezeigt, um anzuzeigen, dass dieses Konto deaktiviert ist.

Configuring The SNMP Agent

Server Administrator supports the Simple Network Management Protocol (SNMP—a systems management standard—on all supported operating systems. The SNMP support may or may not be installed depending on your operating system and how the operating system was installed. In most cases, SNMP is installed as part of your operating system installation. An installed supported systems management protocol standard, such as SNMP, is required before installing Server Administrator.

You can configure the SNMP agent to change the community name and to send traps to a management station. To configure your SNMP agent for proper interaction with management applications such as the Dell OpenManage Essentials, perform the procedures described in the following sections.



NOTE: The default SNMP agent configuration usually includes a SNMP community name such as public. For security reasons, you must rename the default SNMP community names. For information about renaming the SNMP community names, see Changing The SNMP Community Name.



NOTE: For IT Assistant to retrieve management information from a system running Server Administrator, the community name used by IT Assistant must match a community name on the system running Server Administrator. For IT Assistant to modify information or perform actions on a system running Server Administrator, the community name used by IT Assistant must match a community name that allows Set operations on the system running Server Administrator. For IT Assistant to receive traps (asynchronous event notifications) from a system running Server Administrator, the system running Server Administrator must be configured to send traps to the system running IT Assistant.

The following procedures provide step-by-step instructions for configuring the SNMP agent for each supported operating system:

- Configuring the SNMP Agent For Systems Running Supported Windows Operating Systems
- Configuring the SNMP Agent On Systems Running Supported Red Hat Enterprise Linux
- Configuring the SNMP Agent On Systems Running Supported SUSE Linux Enterprise Server
- Configuring the SNMP Agent on Systems Running Supported VMware ESXi 5.X and ESXi 6.X Operating Systems

Konfigurieren von SNMP-Agenten für Systeme, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden

Der Server Administrator verwendet die SNMP-Dienste, die vom Windows SNMP-Agenten bereitgestellt werden. Sie können den SNMP-Agenten zur Änderung des Community-Namens und zum Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie dem IT Assistant führen Sie die im Folgenden beschriebenen Verfahren aus.



ANMERKUNG: Weitere Informationen zur SNMP-Konfiguration finden Sie in der Betriebssystem-Dokumentation.

SNMP-Community-Namen ändern

 ANMERKUNG: Sie können die SNMP-Community-Namen von Server Administrator einstellen. Legen Sie den Community-Namen unter Verwendung der Betriebssystem-SNMP-Tools fest.

Durch die Konfiguration der SNMP-Community-Namen wird festgelegt, welche Systeme das System über SNMP verwalten können. Der von Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem System, auf dem Server Administrator ausgeführt wird, konfiguriert wurde, sodass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.

1. Öffnen Sie das Fenster **Computerverwaltung**.
2. Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.
3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienste** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften**.

   Das Fenster **SNMP-Diensteinstellungen** wird deaktiviert.
5. Klicken Sie auf das Register **Sicherheit**, um einen Community-Namen hinzuzufügen oder zu ändern.

   So fügen Sie einen Community-Namen hinzu:

   a. Klicken Sie in der Liste **Akzeptierte Community-Namen** auf **Hinzufügen**.

      Das Fenster **SNMP-Dienstkonfiguration** wird eingeblendet.
   b. Geben Sie in das Feld **Community-Name** den Community-Namen eines Systems ein, das Ihr System verwalten kann (die Standardeinstellung ist öffentlich) und klicken Sie auf **Hinzufügen.**

      Das Fenster **SNMP-Diensteigenschaften** wird eingeblendet.

   So bearbeiten Sie einen Community-Namen:

   a. Wählen Sie einen Community-Namen aus der Liste **Akzeptierte Community-Namen** aus, und klicken dann Sie auf **Bearbeiten**.

      Das Fenster **SNMP-Dienstkonfiguration** wird eingeblendet.
   b. Bearbeiten Sie den Community-Namen im Feld **Community-Name** und klicken Sie auf **OK**.

      Das Fenster **SNMP-Diensteigenschaften** wird eingeblendet.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Konfigurieren des Systems zum Senden von SNMP-Traps an eine Management Station

Server Administrator erzeugt SNMP-Traps als Reaktion auf Statusänderungen der Sensoren und anderer überwachter Parameter. Sie müssen ein oder mehrere Trap-Ziele auf dem Server Administrator ausführenden System konfigurieren, um SNMP-Traps an eine Verwaltungsstation zu senden.

1. Öffnen Sie das Fenster **Computerverwaltung**.
2. Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.
3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienst** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften**.

   Das Fenster **Eigenschaften von SNMP-Dienst** wird eingeblendet.
5. Klicken Sie auf das Register **Traps**, um eine Community für Traps hinzuzufügen oder um ein Trap-Ziel für eine Trap-Community hinzuzufügen.

   a. Geben Sie zum Hinzufügen einer Community für Traps den Community-Namen im Feld **Community-Name** ein und klicken dann auf **Zur Liste hinzufügen** neben dem Feld **Community-Name** .

b. Wählen Sie zum Hinzufügen eines Trap-Ziels für eine Trap-Community den Community-Namen aus dem Drop-Down-Feld **Community-Name** und klicken Sie auf **Hinzufügen** im Feld **Trap-Ziele**.

   Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

c. Geben Sie im Feld **Host-Name**, **IP- oder IPX-Adresse** das Trap-Ziel ein, **Hinzufügen**.

   Das Fenster **Eigenschaften von SNMP-Dienst** wird eingeblendet.

6. Klicken Sie zum Speichern der Änderungen auf **OK**.

SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden

Server Administrator verwendet die SNMP-Dienste, die vom **net-snmp**-Agenten bereitgestellt werden. Sie können den SNMP-Agenten zur Änderung des Community-Namens, zur Aktivierung von Set-Vorgängen und zum Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie dem IT Assistant führen Sie die im Folgenden beschriebenen Verfahren aus.

 ANMERKUNG: Weitere Informationen zur SNMP-Konfiguration finden Sie in der Dokumentation zum Betriebssystem.

Konfiguration von SNMP-Agent Access Control

Der Zweig der Verwaltungsinformationsbasis (MIB), der vom Server Administrator implementiert wird, wird mit dem Objektbezeichner (OID) 1.3.6.1.4.1.674 gekennzeichnet. Verwaltungsanwendungen müssen Zugriff auf diesen Zweig der MIB-Struktur besitzen, um Systeme verwalten zu können, die Server Administrator ausführen.

Bei Red Hat Enterprise Linux- und VMware ESXi 4.0-Betriebssystemen gewährt die standardmäßige SNMP-Agent-Konfiguration Nur-Lese-Zugriff für die *öffentliche* Community nur an den *System*-Zweig MIB-II (gekennzeichnet mit der OID 1.3.6.1.2.1.1) der MIB-Struktur. Diese Konfiguration lässt nicht zu, dass Verwaltungsanwendungen Informationen von Server Administrator oder andere Systems Management-Informationen außerhalb des *System*-Zweigs MIB-II abrufen oder ändern.

Server Administrator SNMP Agent - Installationsmaßnahmen

Wenn Server Administrator die standardmäßige SNMP-Konfiguration während der Installation ermittelt, versucht die Anwendung, die SNMP-Agent-Konfiguration so zu ändern, dass die gesamte MIB-Struktur für die öffentliche Community Nur-Lese-Zugriff erhält. Server Administrator ändert die SNMP-Agent-Konfigurationsdatei /etc/snm, p/snmpd.conf durch:

- Erstellen der Ansicht auf die gesamte MIB-Struktur durch Hinzufügen der folgenden Zeile, falls diese noch nicht existiert: `view all included`
- Andern der Zeile für den standardmäßigen Zugriff, so dass die öffentliche Community Nur-Lese-Zugriff auf die gesamte MIB-Struktur erhält. Der Server Administrator sucht die folgende Zeile: `access notConfigGroup "" any noauth exact systemview none none`
- Wenn der Server Administrator die obenstehende Zeile findet, dann ändert er sie folgendermaßen ab: `access notConfigGroup "" any noauth exact all none none`

   ANMERKUNG: Damit sichergestellt ist, dass Server Administrator die SNMP-Agent-Konfiguration ändern kann, um korrekten Zugriff auf die Systems Management-Daten zu gewähren, wird empfohlen, etwaige weitere SNMP-Agent-Konfigurationsänderungen erst nach Installation von Server Administrator vorzunehmen.

Server Administrator-SNMP kommuniziert mit dem SNMP-Agenten über das SNMP-Multiplexing-Protokoll (SMUX). Wenn das Server Administrator-SNMP mit dem SNMP-Agenten eine Verbindung

herstellt, sendet es einen Objektbezeichner an den SNMP-Agenten, um sich als SMUX-Peer zu identifizieren. Da dieser Objektbezeichner mit dem SNMP-Agenten konfiguriert werden muss, fügt Server Administrator der Konfigurationsdatei /etc/snmp/snmpd.conf des SNMP-Agenten während der Installation die folgende Zeile hinzu, wenn diese nicht vorhanden ist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

SNMP-Community-Namen ändern

Die Konfiguration des SNMP-Community-Namens bestimmt, welche Systeme das System über SNMP verwalten können. Der von Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-System konfiguriert wurde, sodass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.
Zum Ändern des SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen von einem System verwendet wird, auf dem Server Administrator ausgeführt wird:

1. Öffnen Sie die Datei SNMP-Agentenkonfiguration /etc/snmp/snmpd.conf.
2. Suchen Sie folgende Zeile: `com2sec publicsec default public` oder `com2sec notConfigUser default public.`

   ANMERKUNG: Suchen Sie folgende Zeile für IPv6, `com2sec6 notConfigUser default public`. Fügen Sie auch den Text `agentaddress udp6:161` der Datei hinzu:.
3. Bearbeiten Sie diese Zeile und ersetzen Sie `public` durch den neuen SNMP-Community-Namen. Nach der Bearbeitung muss die Zeile wie folgt aussehen: `com2sec publicsec default community_name` oder `com2sec notConfigUser default community_name.`
4. Starten Sie zur Aktivierung von Änderungen der SNMP-Konfiguration den SNMP-Agenten neu durch Eingabe von: `service snmpd restart`.

Konfigurieren des Systems zum Senden von Traps an eine Management Station

Server Administrator erzeugt SNMP-Traps als Reaktion auf Statusänderungen der Sensoren und anderer überwachter Parameter. Sie müssen ein oder mehrere Trap-Ziele auf dem Server Administrator ausführenden System konfigurieren, um SNMP-Traps an eine Management Station zu senden.

Um das System, auf dem Server Administrator ausgeführt wird, so zu konfigurieren, dass Traps an eine Management Station gesendet werden, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei, /etc/snmp/snmpd.conf und führen die folgenden Schritte aus:

1. Fügen Sie folgende Zeile der Datei hinzu: `trapsink IP_address community_name`, wobei `IP_address` die IP-Adresse der Management Station ist und `community_name` derSNMP-Community-Name ist.
2. Starten Sie zur Aktivierung von Änderungen der SNMP-Konfiguration den SNMP-Agenten neu durch Eingabe von: `service snmpd restart`.

SNMP-Agent auf Systemen konfigurieren, auf denen der unterstützte SUSE Linux Enterprise Server ausgeführt wird

Server Administrator verwendet die SNMP-Dienste, die vom net-snmp-Agenten bereitgestellt werden. Sie können den SNMP-Agenten so konfigurieren, dass der SNMP-Zugriff über Remote-Hosts aktiviert ist, der Community-Name geändert werden kann, SNMP-Set-Vorgänge aktiviert sind und Traps an eine Management Station gesendet werden. Führen Sie zur Konfiguration des SNMP-Agenten für korrekte Interaktion mit Verwaltungsanwendungen wie z. B. IT Assistant die im Folgenden beschriebenen Verfahren durch.

 ANMERKUNG: Weitere Informationen zur SNMP-Konfiguration finden Sie in der Betriebssystem-Dokumentation.

SNMP-Installationsmaßnahme für Server Administrator

Server Administrator-SNMP kommuniziert mit dem SNMP-Agenten unter Verwendung des SMUX-Protokolls. Wenn das Server Administrator-SNMP mit dem SNMP-Agenten eine Verbindung herstellt, sendet es einen Objektbezeichner an den SNMP-Agenten, um sich als SMUX-Peer zu identifizieren. Da dieser Objektbezeichner mit dem SNMP-Agenten konfiguriert werden muss, fügt Server Administrator der SNMP-Agent-Konfigurationsdatei während der Installation die Zeile **/etc/snmp/snmpd.conf** hinzu, falls diese nicht vorhanden ist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

SNMP-Zugang von Remote-Hosts aktivieren

Die Standard-SNMP Agent-Konfiguration auf SUSE Linux Enterprise Server-Betriebssystemen erteilt Nur-Lese-Zugriff auf die komplette MIB-Struktur an die öffentliche Community ausschließlich vom lokalen Host. Diese Konfiguration lässt keine SNMP-Verwaltungsanwendungen wie IT Assistant, die auf anderen Hosts ausgeführt werden, für eine einwandfreie Erkennung und Verwaltung von Server Administrator-Systemen zu. Wenn Server Administrator diese Konfiguration während der Installation feststellt, protokolliert er eine Meldung für die Betriebssystem-Protokolldatei, /var/log/messages, um anzuzeigen, dass der SNMP-Zugriff auf den lokalen Host beschränkt ist. Sie müssen den SNMP-Agenten konfigurieren, um den SNMP-Zugang von Remote-Hosts zu aktivieren, wenn Sie das System mit SNMP-Verwaltungsanwendungen von Remote-Hosts aus verwalten möchten.

 ANMERKUNG: Aus Sicherheitsgründen ist es ratsam, den SNMP-Zugriff auf bestimmte Remote-Hosts soweit wie möglich einzuschränken.

Um den SNMP-Zugriff über einen bestimmten Remote-Host auf ein System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei /etc/snmp/snmpd.conf und führen die folgenden Schritte durch:

1. Suchen Sie folgende Zeile: `rocommunity public 127.0.0.1`.
2. Bearbeiten oder kopieren Sie diese Zeile und ersetzen Sie 127.0.0.1 mit der IP-Adresse des Remote-Hosts. Nach der Bearbeitung muss die Zeile wie folgt aussehen: `rocommunity public IP_address`.

   ANMERKUNG: Sie können SNMP-Zugriff von mehreren spezifischen Remote-Hosts aktivieren, indem Sie eine `rocommunity`-Direktive für jeden Remote-Host hinzufügen.
3. Zur Aktivierung von Änderungen der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von: `/etc/init.d/snmpd restart`

   Um den SNMP-Zugriff über alle Remote-Hosts auf ein System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei /etc/snmp/snmpd.conf und führen die folgenden Schritte durch:
4. Suchen Sie folgende Zeile: `rocommunity public 127.0.0.1`.
5. Bearbeiten Sie diese Zeile, indem Sie 127.0.0.1 löschen. Nach der Bearbeitung muss die Zeile wie folgt aussehen: `rocommunity public`.
6. Zur Aktivierung von Änderungen der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von: `/etc/init.d/snmpd restart`

SNMP-Community-Namen ändern

Die Konfiguration des SNMP-Community-Namens bestimmt, welche Management Stations das System über SNMP verwalten kann. Der von Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem System aktiviert wurde, auf dem Server Administrator ausgeführt wird, sodass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.

Zum Ändern des standardmäßigen SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen über ein System verwendet wird, das Server Administrator ausführt:

1. Öffnen Sie die SNMP-Agentenkonfigurationsdatei **/etc/snmp/snmpd.conf**.
2. Suchen Sie folgende Zeile: `rocommunity public 127.0.0.1.`
3. Bearbeiten Sie diese Zeile, indem Sie `public` durch den neuen SNMP-Community-Namen ersetzen. Nach der Bearbeitung muss die Zeile wie folgt aussehen: `rocommunity community_name 127.0.0.1.`
4. Starten Sie zur Aktivierung von Änderungen der SNMP-Konfiguration den SNMP-Agenten neu durch Eingabe von: **/etc/init.d/snmpd restart**.

Konfigurieren des SNMP-Agenten auf Systemen, die unterstützte VMware ESXi 5.X- und ESXi 6X-Betriebssysteme ausgeführt werden

Server Administrator unterstützt SNMP-Traps auf VMware ESXi 5.X und ESXi 6.X. Wenn nur eine eigenständige Lizenz vorhanden ist, schlägt die SNMP-Konfiguration auf VMware ESXi-Betriebssystemen fehl. Server Administrator unterstützt keine SNMP-Get- und -Set-Vorgänge auf VMWare ESXi 5.X und ESXi 6.X, da die erforderliche SNMP-Unterstützung nicht verfügbar ist. Die VMware vSphere-CLI (Befehlszeilenoberfläche) wird verwendet, um Systeme zu konfigurieren, die VMware ESXi 5.X und ESXi 6.X SNMP-Traps an eine Management Station zu senden.



ANMERKUNG: Weitere Informationen zur Verwendung der VMware vSphere-Befehlszeilenschnittstelle finden Sie unter **vmware.com/support**.

Konfigurieren des Systems zum Senden von Traps an eine Management Station

Server Administrator erzeugt SNMP-Traps als Reaktion auf Statusänderungen der Sensoren und anderer überwachter Parameter. Sie müssen ein oder mehrere Trap-Ziele auf dem Server Administrator ausführenden System konfigurieren, um SNMP-Traps an eine Management Station zu senden.

Führen Sie zum Konfigurieren des ESXi-Systems, das Server Administrator zum Senden von Traps an eine Management Station ausführt, die folgenden Schritte aus:

1. Installieren Sie VMware vSphere CLI.
2. Öffnen Sie eine Eingabeaufforderung auf dem System, auf dem die VMware vSphere CLI installiert ist.
3. Wechseln Sie zum Verzeichnis, in dem die VMware vSphere CLI installiert ist. Der Standardspeicherort auf Linux befindet sich unter **/usr/bin**. Der Standardspeicherort auf Windows befindet sich unter **C:\Program Files\VMware\VMware vSphere CLI\bin**.
4. Führen Sie den folgenden Befehl aus: `vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname> @162/<community>`

   Dabei ist `<server>` der Hostname oder die IP-Adresse des ESXi-Systems, `<username>` der Benutzer auf dem ESXi-System, `<community>` der SNMP Community-Name und `<hostname>` der Hostname oder die IP-Adresse der Management Station.

ANMERKUNG: Die Dateierweiterung .pl wird unter Linux nicht benötigt.

ANMERKUNG: Wenn Sie den Benutzernamen und das Kennwort nicht angeben, werden Sie dazu aufgefordert.

Die SNMP-Trap-Konfiguration wird sofort ohne Neustart von Diensten wirksam.

Firewall-Konfiguration auf Systemen, die unterstützte Red Hat Enterprise Linux-Betriebssysteme und SUSE Linux Enterprise Server ausführen

Wenn Sie beim Installieren von Red Hat Enterprise Linux/SUSE Linux die Firewall-Sicherheit aktivieren, wird die SNMP-Schnittstelle an allen externen Netzwerkschnittstellen standardmäßig geschlossen. Damit SNMP-Verwaltungsanwendungen wie IT Assistant Informationen von Server Administrator ermitteln und empfangen können, muss die SNMP-Schnittstelle auf mindestens einer externen Netzwerkschnittstelle geöffnet sein. Wenn der Server Administrator ermittelt, dass keine SNMP-Schnittstelle in der Firewall für eine externe Netzwerkschnittstelle geöffnet ist, zeigt der Server Administrator eine Warnmeldung an und trägt eine Meldung in das Systemprotokoll ein.

Um den SNMP-Anschluss zu öffnen, muss die Firewall deaktiviert, eine gesamte externe Netzwerkschnittstelle der Firewall geöffnet oder der SNMP-Anschluss von mindestens einer externen Netzwerkschnittstelle der Firewall geöffnet werden. Diese Maßnahme kann vor oder nach dem Start des Server Administrators durchgeführt werden.

Um die SNMP-Schnittstelle auf Red Hat Enterprise Linux mittels einer der zuvor beschriebenen Methoden zu öffnen, führen Sie die folgenden Schritte durch:

1. Geben Sie bei der Befehlsaufforderung von Red Hat Enterprise Linux den Befehl `setup` ein und drücken Sie <Eingabe>, um das Textmodus-Setup-Dienstprogramm zu starten.

   ANMERKUNG: Dieser Befehl steht nur dann zur Verfügung, wenn das Betriebssystem mit Standardeinstellungen installiert worden ist.

   Das Menü **Hilfsprogramm auswählen** wird eingeblendet.
2. Wählen Sie **Firewall-Konfiguration** mit dem Nach-unten-Pfeil aus und drücken Sie die Eingabetaste.

   Der Bildschirm **Firewall-Konfiguration** wird geöffnet.
3. Drücken Sie die Tabulatortaste, um **Sicherheitsstufe** auszuwählen, und drücken Sie die Leertaste, um die Sicherheitsstufe auszuwählen, die Sie einstellen möchten. Die ausgewählte **Sicherheitsstufe** wird mit einem Sternchen markiert.

   ANMERKUNG: Drücken Sie die Taste <F1>, um weitere Informationen über die Sicherheitsstufen der Firewall zu erhalten. Die Standard-SNMP-Anschlussnummer ist 161. Wenn Sie die grafische Benutzeroberfläche von X Window System verwenden, dann kann es sein, dass bei neueren Versionen von Red Hat Enterprise Linux durch Drücken von <F1> die Informationen über die Firewall-Sicherheitsstufen nicht angezeigt werden.

   a. Wählen Sie zur Deaktivierung der Firewall die Optionen **Keine Firewall** oder **Deaktiviert** aus und gehen dann zu Schritt 7.
   b. Zum Öffnen einer ganzen Netzwerkschnittstelle oder der SNMP-Schnittstelle wählen Sie **Hoch, Mittel** oder **Aktiviert** und fahren Sie mit Schritt 4 fort.
4. Drücken Sie die <Tabulatortaste>, um zum Anpassen zu wechseln, und drücken Sie die <Eingabe>-Taste.

   Der Bildschirm **Firewall-Konfiguration - Anpassen** wird geöffnet.
5. Wählen Sie aus, ob eine gesamte Netzwerkschnittstelle oder nur eine SNMP-Schnittstelle auf allen Netzwerkschnittstellen geöffnet werden soll.

a. Um eine gesamte Netzwerkschnittstelle zu öffnen, wechseln Sie mit der Tabulatortaste zu einer vertrauenswürdigen Komponente und drücken Sie die Leertaste. Ein Sternchen im Feld links neben dem Gerätenamen zeigt an, dass die gesamte Schnittstelle geöffnet ist.
b. Um eine SNMP-Schnittstelle auf allen Netzwerkschnittstellen zu öffnen, wechseln Sie mit der Tabulatortaste zu „Weitere Schnittstellen“ und geben Sie `snmp:udp` ein.

6. Drücken Sie die **Tabulatortaste**, um **OK** auszuwählen, und drücken Sie die **Eingabetaste**

   Der Bildschirm **Firewall-Konfiguration** wird geöffnet.
7. Drücken Sie die **Tabulatortaste**, um **OK** auszuwählen, und drücken Sie die **Eingabetaste**

   Das Menü **Hilfsprogramm auswählen** wird eingeblendet.
8. Drücken Sie die **Tabulatortaste**, um **Beenden** auszuwählen, und drücken Sie die **Eingabetaste**.

Firewall-Konfiguration

Um die SNMP-Schnittstelle auf SUSE Linux Enterprise Server zu öffnen:

1. Konfigurieren Sie SuSEfirewall2, indem Sie auf einer Konsole Folgendes ausführen: `a.# yast2 firewall`
2. Verwenden Sie die Pfeiltasten, um zu **Zulässige Dienste** zu wechseln.
3. Drücken Sie auf <Alt><d>, um das Dialogfeld **Zusätzliche zulässige Schnittstellen** zu öffnen.
4. Drücken Sie auf <Alt><T>, um den Cursor zum Textfeld **TCP-Schnittstellen** zu bewegen.
5. Geben Sie **snmp** in das Textfeld ein.
6. Drücken Sie auf <Alt><O> <Alt><N>, um zum nächsten Bildschirm zu wechseln.
7. Drücken Sie auf <Alt><A>, um die Änderungen zu akzeptieren und sie zu übernehmen.

3

Server Administrator verwenden

Klicken Sie zum Starten einer Server Administrator-Sitzung doppelt auf das Symbol **Server Administrator** auf dem Desktop.

Daraufhin wird der Bildschirm **Server Administrator-Anmeldung** angezeigt. Die Standardschnittstelle für Server Administrator ist 1311. Falls erforderlich, können Sie die Schnittstelle ändern. Anleitungen zum Einrichten der Systemeinstellungen finden Sie unter Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup.



ANMERKUNG: Server, die auf XenServer 6.0 ausgeführt werden, können über die Befehlszeilenschnittstelle (CLI) oder einen zentralen Webserver verwaltet werden, der auf einem separaten Rechner installiert ist.

An- und Abmelden

Sie können sich auf die folgenden Weisen bei Server Administrator anmelden:

- Server Administrator, Lokales System-Anmeldung
- Server Administrator Managed System-Anmeldung – unter Verwendung des Desktop-Symbols
- Server Administrator Managed System-Anmeldung – unter Verwendung des Webbrowsers
- Zentrale Web Server-Anmeldung

Server Administrator, Lokales System-Anmeldung

Diese Art der Anmeldung ist nur verfügbar, wenn Sie die Server Instrumentation- und Server Administrator Web Server-Komponenten auf dem lokalen System installieren.



ANMERKUNG: Diese Option ist für Server, die auf XenServer 6.0 ausgeführt werden, nicht verfügbar.

So melden Sie sich bei Server Administrator auf einem lokalen System an:

1. Geben Sie Ihren zugewiesenen **Benutzernamen** und Ihr **Kennwort** in die entsprechenden Felder des Systems Management-**Anmeldungs**fensters ein.

   Wenn Sie über eine definierte Domäne auf Server Administrator zugreifen, müssen Sie auch den korrekten Domänennamen angeben.
2. Wählen Sie das Kontrollkästchen für **Active Directory-Anmeldung** aus, um sich unter Verwendung von Microsoft Active Directory anzumelden. Finden Sie Active Directory-Anmeldung verwenden.
3. Klicken Sie auf **Senden**.

Um die Server Administrator-Sitzung zu beenden, klicken Sie auf die Schaltfläche **Abmelden** oben rechts auf der Startseite von jedem **Server Administrator**.

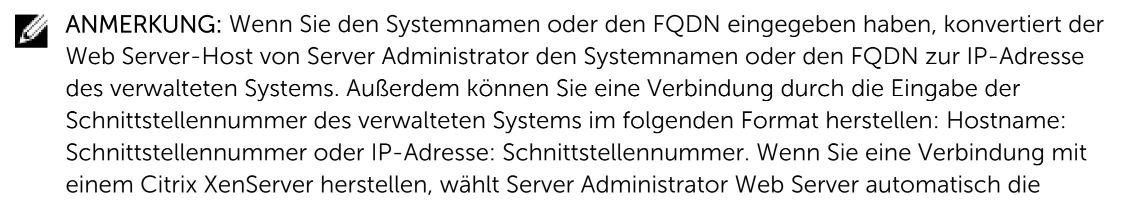


ANMERKUNG: Weitere Informationen zum Konfigurieren des Active Directory auf Systemen, die CLI verwenden, finden Sie im *Management Station Software Installation Guide* (Management Station Software-Installationshandbuch) unter dell.com/openmanagemanuals.

Server Administrator Managed System-Anmeldung – unter Verwendung des Desktop-Symbols

Diese Art der Anmeldung ist nur verfügbar, wenn die Server Administrator Web Server-Komponente auf dem System installiert ist. So melden Sie sich bei Server Administrator an, um ein Remote-System zu verwalten:

1. Klicken Sie doppelt auf das Symbol **Server Administrator** auf Ihrem Desktop.
2. Geben Sie die IP-Adresse oder den Systemnamen oder den vollständigen qualifizierten Domänennamen (FQDN) des Managed System ein.



ANMERKUNG: Wenn Sie den Systemnamen oder den FQDN eingegeben haben, konvertiert der Web Server-Host von Server Administrator den Systemnamen oder den FQDN zur IP-Adresse des verwalteten Systems. Außerdem können Sie eine Verbindung durch die Eingabe der Schnittstellennummer des verwalteten Systems im folgenden Format herstellen: Hostname: Schnittstellennummer oder IP-Adresse: Schnittstellennummer. Wenn Sie eine Verbindung mit einem Citrix XenServer herstellen, wählt Server Administrator Web Server automatisch die Standardschnittstelle (5986) aus, oder Sie können eine andere Schnittstelle festlegen.

3. Wenn Sie eine Intranet-Verbindung verwenden, wählen Sie das Kontrollkästchen **Zertifikatswarnungen ignorieren** aus.
4. Wählen Sie **Active Directory-Anmeldung** aus, um sich unter Verwendung von Microsoft Active Directory Authentifizierung anzumelden. Wenn Sie keine Active Directory-Software benutzen, um den Zugriff auf Ihr Netzwerk zu steuern, wählen Sie nicht **Active Directory-Anmeldung**. Siehe Active Directory-Anmeldung verwenden.
5. Klicken Sie auf **Senden**.

Server Administrator Managed System-Anmeldung – unter Verwendung des Webbrowsers



ANMERKUNG: Sie müssen bereits zugewiesene Benutzer-Zugriffsrechte haben, um sich bei Server Administrator anmelden zu können. Anleitungen zur Einrichtung von neuen Benutzern finden Sie unter Setup und Administration.

1. Öffnen Sie den Webbrowser.
2. Geben Sie eine der folgenden Eingaben in das Feld „Adresse“ ein:
   - `https://hostname:1311`, wobei Hostname der zugewiesene Name des verwalteten Knotensystems ist und 1311 die Standardschnittstellennummer.
   - `https://IP address:1311`, wobei IP-Adresse die IP-Adresse für das verwaltete System ist und 1311 die Standardschnittstellennummer.

   ANMERKUNG: Vergewissern Sie sich, dass Sie `https://` (und nicht `http://`) in das Feld „Adresse“ eingeben.
3. Drücken Sie die <Eingabetaste>.

Zentrale Web Server-Anmeldung

Diese Art der Anmeldung ist nur verfügbar, wenn die Server Administrator Web Server-Komponente auf dem System installiert ist. Verwenden Sie diese Anmeldung, um den zentralen Web Server von Server Administrator zu verwalten:

1. Klicken Sie doppelt auf das Symbol **Server Administrator** auf Ihrem Desktop. Die Seite „Remote-Anmeldung" wird angezeigt.

   VORSICHT: Auf dem Anmeldebildschirm befindet sich das Kontrollkästchen Zertifikatswarnungen ignorieren. Verwenden Sie diese Option mit Vorsicht. Es wird empfohlen, diese Option nur in vertrauenswürdigen Intranet-Umgebungen zu verwenden.
2. Klicken Sie auf den Link **Webserver verwalten** oben rechts auf dem Bildschirm.
3. Geben Sie den **Benutzernamen, das Kennwort** und den **Domänennamen** ein (wenn Sie über eine definierte Domäne auf Server Administrator zugreifen), und klicken Sie auf **Senden**.
4. Wählen Sie das Kontrollkästchen für **Active Directory-Anmeldung** unter Verwendung von Microsoft Active Directory aus. Siehe Die Active Directory-Anmeldung verwenden.
5. Klicken Sie auf **Senden**.

   Klicken Sie zum Beenden der Server Administrator-Sitzung auf **Abmelden** auf der Allgemeinen Navigationsleiste.

   ANMERKUNG: Wenn Sie Server Administrator unter Verwendung von Mozilla Firefox Version 3.0 und 3.5 oder Microsoft Internet Explorer Version 7.0 oder 8.0 starten, erscheint eventuell eine zwischengeschaltete Warnungsseite, auf der ein Problem mit dem Sicherheitszertifikat angezeigt wird. Zur Gewährleistung der Systemsicherheit wird dringend empfohlen, entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wiederzuverwenden oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) zu importieren. Um solche Warnungsmeldungen über das Zertifikat zu vermeiden, muss das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammen. Weitere Informationen über X.509-Zertifikatsverwaltung erhalten Sie unter X.509-Zertifikatsverwaltung.

   ANMERKUNG: Um die Systemsicherheit zu gewährleisten, empfiehlt Dell, eine Zertifikatskette von einer Zertifizierungsstelle (CA) zu importieren. Weitere Informationen finden Sie in der VMware-Dokumentation.

   ANMERKUNG: Wenn die Zertifizierungsstelle auf dem verwalteten System gültig ist und der Server Administrator-Webserver noch immer einen nicht vertrauensunwürdigen Zertifikatsfehler meldet, können Sie durch die Verwendung der Datei certutil.exe die Zertifizierungsstelle des verwalteten Systems trotzdem als vertrauenswürdig einstufen. Weitere Informationen zum Zugreifen auf diese .exe Datei finden Sie in Ihrem Handbuch zum Betriebssystem. Auf unterstützten Windows-Betriebssystemen können Sie auch die Option Zertifikat-Snap-In verwenden, um Zertifikate zu importieren.

Die Active Directory-Anmeldung verwenden

Wählen Sie **Active Directory-Anmeldung** aus, um sich unter Verwendung der erweiterten Schemalösung von Dell bei Active Directory anzumelden.

Diese Lösung ermöglicht Ihnen, Zugriff auf Server Administrator zu gewähren. Sie können damit Server Administrator-Benutzer und -Berechtigungen zu bestehenden Benutzern in Ihrer Active Directory-Software hinzufügen bzw. steuern. Weitere Informationen finden Sie unter "Microsoft Active Directory

verwenden" im *Server Administrator Installation Guide* (Installationshandbuch zu Server Administrator) unter dell.com/openmanagemanuals.

Einmaliges Anmelden

Die Option der einfachen Anmeldung auf Windows-Betriebssystemen ermöglicht allen angemeldeten Benutzern, die Anmeldungsseite zu umgehen und durch Klicken auf das **Server Administrator**-Symbol auf dem Desktop auf die Server Administrator-Webanwendung zuzugreifen.



ANMERKUNG: Weitere Informationen zur einfachen Anmeldung finden Sie im Knowledge Base-Artikel unter support.microsoft.com/default.aspx?scid=kb;en-us;Q258063.

Für den Zugriff auf lokale Rechner ist es nicht erforderlich, dass Sie auf der Maschine ein Konto mit entsprechenden Berechtigungen haben (Benutzer, Hauptbenutzer oder Verwalter). Andere Benutzer werden gegen Microsoft Active Directory authentifiziert. Um Server Administrator mit Hilfe von Einfachanmeldungs-Authentifizierung gegen Microsoft Active Directory zu starten, müssen die folgenden Parameter ebenfalls eingereicht werden:

```
authType=ntlm&application=[Plugin-Name]
```

wobei `plugin name = omsa, ita,` usw.

Beispiel:

```
https://localhost:1311/?authType=ntlm&application=omsa
```

Um Server Administrator mit Hilfe von Einfachanmeldungs-Authentifizierung gegen die Benutzerkonten des lokalen Rechners zu starten, müssen die folgenden Parameter ebenfalls eingereicht werden:

```
authType=ntlm&application=[Plugin-Name]&locallogin=true
```

wobei `plugin name = omsa, ita` usw.

Beispiel:

```
https://localhost:1311/?authType=ntlm&application=omsa&locallogin=true
```

Server Administrator wurde auch erweitert, um anderen Produkten (wie z. B. Dell OpenManage Essentials) direkten Zugriff auf Server Administrator-Webseiten zu geben, ohne über die Anmeldeseite gehen zu müssen (wenn Sie aktuell angemeldet sind und die erforderlichen Berechtigungen haben).

Konfiguration von Sicherheitseinstellungen auf Systemen, die ein unterstütztes Microsoft Windows-Betriebssystem ausführen

Sie müssen die Sicherheitseinstellungen für Ihren Browser so konfigurieren, dass die Anmeldung am Server Administrator über ein Remote-Verwaltungssystem erfolgt, das ein unterstütztes Microsoft Windows-Betriebssystem ausführt.

Die Sicherheitseinstellungen für den Browser verhindern auf der Client-Seite möglicherweise die Ausführung von Skripts, die von Server Administrator verwendet werden. Um Skripts auf der Client-Seite zu aktivieren, führen Sie folgende Schritte auf dem Remote-Verwaltungssystem durch.

ANMERKUNG: Wenn der Browser nicht für die Verwendung von Skripts auf der Client-Seite konfiguriert wurde, wird bei der Anmeldung bei Server Administrator möglicherweise ein leerer Bildschirm angezeigt. In diesem Fall wird eine Fehlermeldung ausgegeben mit der Anweisung, die Browsereinstellungen zu konfigurieren.

Aktivieren der Skripts auf der Client-Seite auf Internet Explorer

1. Klicken Sie im Webbrowser auf **Extras** → **Internetoptionen** → **Sicherheit**.
   Das Fenster **Internetoptionen** wird angezeigt.
2. Klicken Sie unter **Wählen Sie eine Zone aus, um deren Sicherheitseinstellungen festzulegen**, auf **Vertrauenswürdige Sites**, und dann auf **Sites**.
3. Geben Sie in das Feld **Diese Website zur Zone hinzufügen** die Webadresse für den Zugriff auf das verwaltete Remote-System ein.
4. Klicken Sie auf **Hinzufügen**.
5. Kopieren Sie die Webadresse für den Zugriff auf das verwaltete Remote-System von der Adresszeile des Browsers und fügen Sie die Adresse im Feld **Diese Website der Zone hinzufügen** ein.
6. Klicken Sie dann unter **Sicherheitsstufe dieser Zone** auf **Benutzerdefinierte** Stufe.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.
8. Schließen Sie den Browser, und melden Sie sich beim Server Administrator an.

Einfache Anmeldung For Server Administrator On Internet Explorer aktivieren

Um einfache Anmeldung für Server Administrator ohne Eingabeaufforderung für Benutzeranmeldeinformationen zuzulassen:

1. Klicken Sie im Webbrowser auf **Extras** → **Internetoptionen** → **Sicherheit** .
2. Klicken Sie unter **Wählen Sie eine Zone aus, um deren Sicherheitseinstellungen festzulegen**, auf **Vertrauenswürdige Sites**, und dann auf **Sites**.
3. Geben Sie in das Feld **Diese Website zur Zone hinzufügen** die Webadresse für den Zugriff auf das verwaltete Remote-System ein.
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Stufe anpassen**.
6. Unter **Benutzerauthentifizierung** wählen Sie **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** aus.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.
8. Schließen Sie den Browser, und melden Sie sich beim Server Administrator an.

Aktivierung der Verwendung von Client-seitigen Skripts auf Mozilla Firefox

1. Öffnen Sie Ihren Browser.
2. Klicken Sie auf **Bearbeiten** → **Voreinstellungen** .
3. Klicken Sie auf **Erweitert** → **Skripts und Plug-ins**.
4. Stellen Sie sicher, dass Navigator unter „JavaScript aktivieren für" ausgewählt ist. Stellen Sie sicher, dass das **Navigator**-Kontrollkästchen unter **JavaScript aktivieren für** markiert ist.
5. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.
6. Schließen Sie den Browser.
7. Melden Sie sich bei Server Administrator an.

Server Administrator-Startseite

 ANMERKUNG: Verwenden Sie Ihre Web Browser-Symbolleistenschaltfläche (z.B. **Zurück** und **Aktualisieren**) nicht, während Sie Server Administrator verwenden. Verwenden Sie nur die Navigationselemente von Server Administrator.

Mit wenigen Ausnahmen besteht die Server Administrator-Startseite aus drei Hauptbereichen:

- Die Allgemeine Navigationsleiste stellt Verknüpfungen zu allgemeinen Diensten zur Verfügung.
- Mittels der Systemstruktur können alle sichtbaren Systemobjekte entsprechend der Zugriffsberechtigungen des Benutzers angezeigt werden.
- Das Maßnahmenfenster zeigt die verfügbaren Verwaltungsmaßnahmen für das gewählte Systemstrukturobjekt an, basierend auf den Zugriffsrechten des Benutzers. Das Maßnahmenfenster enthält drei Funktionsbereiche:
  - In den Maßnahmenregistern werden die primären Maßnahmen oder Maßnahmenkategorien angezeigt, die für das gewählte Systemstrukturobjekt entsprechend den Zugriffsrechten des Benutzers verfügbar sind.
  - Die Maßnahmenregister sind aufgeteilt in Unterkategorien aller verfügbaren sekundären Optionen für die Maßnahmenregister, basierend auf den Zugriffsrechten des Benutzers.
  - Im Datenbereich werden Informationen für das ausgewählte Systemstrukturobjekt, Maßnahmenregister und Unterkategorie entsprechend den Zugriffsrechten des Benutzers angezeigt.

Wenn man bei der **Server Administrator**-Startseite angemeldet ist, werden darüber hinaus das Systemmodell, der zugewiesene Systemname und der Benutzername des gegenwärtigen Benutzers sowie die Benutzerberechtigungen in der oberen rechten Ecke des Fensters angezeigt.

In der folgenden Tabelle listet die Feldnamen der **GUI** und das zutreffende System auf, wenn Server Administrator auf dem System installiert ist.

Tabelle 6. Die Feldnamen der GUI und das zutreffende System

Feldname der Benutzeroberfläche	Entsprechendes System
Modulares Gehäuse	Modulares System
Servermodul	Modulares System
Hauptsystem	Modulares System
System	Nicht modulares System
Hauptsystemgehäuse	Nicht modulares System

Die folgende Abbildung zeigt ein Beispiel-Layout für die Server Administrator-Startseite für einen mit Administratorrechten angemeldeten Benutzer.

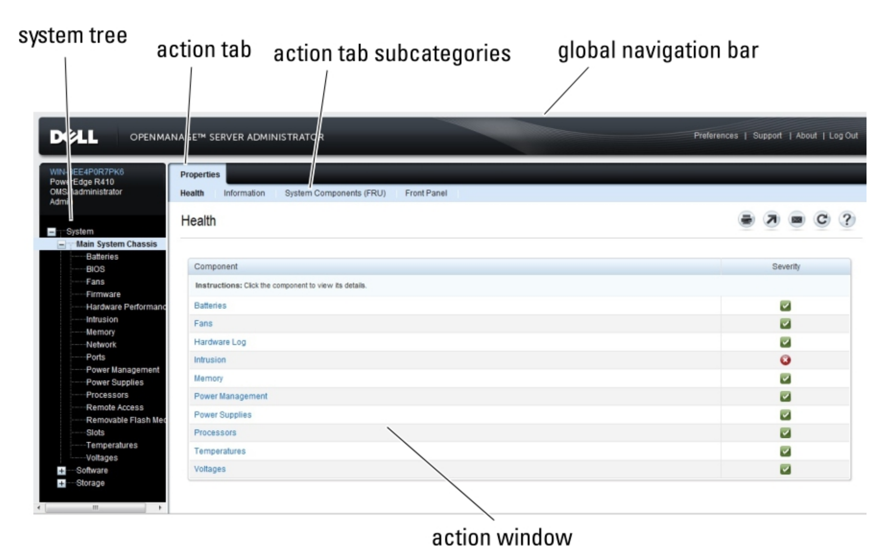


Abbildung 1. Beispielstartseite von Server Administrator - nicht modulares System

Die folgende Abbildung zeigt ein Beispiel-Layout für die Server Administrator-Startseite für einen mit Administratorrechten angemeldeten Benutzer auf einem modularen System.

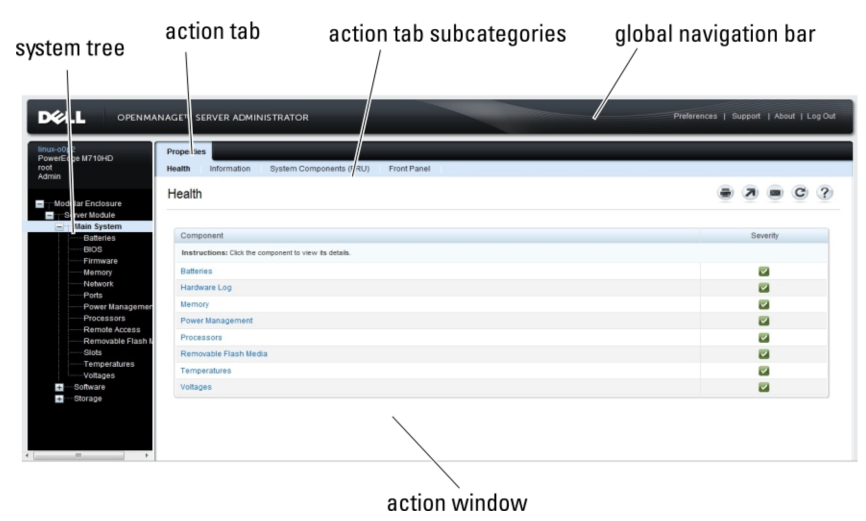


Abbildung 2. Beispielstartseite von Server Administrator - modulares System

Durch Klicken auf ein Objekt in der Systemstruktur wird ein entsprechendes Maßnahmenfenster für das Objekt geöffnet. Sie können durch Klicken auf das Maßnahmenregister zur Auswahl von Hauptkategorien in das Maßnahmenfenster wechseln und auf die Maßnahmenregister-Unterkategorien klicken, um Zugriff auf weiterführende Informationen oder spezifischere Maßnahmen zu erhalten. Die im Datenbereich des Maßnahmenfensters angezeigten Informationen können von Systemprotokollen über Statusanzeigen bis hin zu Systemsondenanzeigen reichen. Im Datenbereich des Maßnahmenfensters unterstrichene Elemente zeigen eine weitere Funktionalitätsebene an. Wenn Sie auf ein unterstrichenes Element klicken, wird dadurch ein neuer Maßnahmenbereich mit mehr Detail im Maßnahmenfenster erstellt. Zum Beispiel wird durch Klicken auf **Hauptsystemgehäuse/Hauptsystem** in der Unterkategorie **Funktionszustand** des Maßnahmenregisters **Eigenschaften** der Zustandsstatus aller im Objekt Hauptsystemgehäuse/ Hauptsystem enthaltenen Komponenten angezeigt, deren Funktionszustand überwacht wird.

ANMERKUNG: Administrator- oder Hauptbenutzer-Zugriffsrechte sind zur Ansicht der meisten der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Zugriffsrechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die **Herunterfahren**-Funktion im Register Herunterfahren.

Unterschiede der Server Administrator-Schnittstellen bei modularen und nicht-modularen Systemen

In der folgenden Tabelle sehen Sie die Verfügbarkeit von Server Administrator-Funktionen für modulare und nicht-modulare Systeme.

Tabelle 7. Unterschiede der Server Administrator-Schnittstellen bei modularen und nicht-modularen Systemen

Funktionen	Modulares System	Nicht modulares System
Batterien	✓	✓
Netzteile	✗	✓
Lüfter	✗	✓
Hardware Performance	✗	✓
Eingriff	✗	✓
Speicher	✓	✓
Netzwerk	✓	✓
Anschlüsse	✓	✓
Stromverwaltung	✓	✓
Prozessoren	✓	✓
Remote-Zugriff	✓	✓
Wechselbarer Flash-Datenträger	✓	✓
Steckplätze	✓	✓
Temperaturen	✓	✓
Spannungen	✓	✓
Modulares Gehäuse (Gehäuse- und CMC-Informationen)	✓	✗

Allgemeine Navigationsleiste

Die allgemeine Navigationsleiste und ihre Verknüpfungen stehen allen Benutzerebenen im Programm zur Verfügung.

- Klicken Sie auf **Einstellungen**, um die Startseite **Einstellungen** zu öffnen. Weitere Informationen finden Sie unter Einstellungen-Startseite verwenden.
- Klicken Sie auf **Support**, um eine Verbindung mit der Dell Support-Website herzustellen.
- Klicken Sie auf **Info**, um die Server Administrator-Version und Copyright-Informationen anzuzeigen.
- Klicken Sie auf **Abmelden**, um die aktuelle Server Administrator-Programmsitzung zu beenden.

Systemstruktur

Die Systemstruktur wird auf der linken Seite der Server Administrator-Startseite angezeigt und enthält die anzeigbaren Komponenten des Systems. Die Systemkomponenten werden nach Komponententyp kategorisiert. Wenn Sie das Hauptobjekt **Modulares Gehäuse** → **System/Servermodul** genannt expandieren, sind die System-/Servermodulkomponenten-Hauptkategorien, die erscheinen können, **Hauptsystemgehäuse/Hauptsystem**, **Software** und **Speicher**.

Um einen Zweig der Struktur zu expandieren, klicken Sie auf das Pluszeichen (+) links neben einem Eintrag, oder doppelklicken Sie auf den Eintrag. Ein Minuszeichen (−) zeigt einen expandierten Eintrag an, der nicht weiter expandiert werden kann.

Maßnahmenfenster

Wenn Sie auf ein Element der Systemstruktur klicken, werden Details über die Komponenten bzw. das Objekt im Datenbereich des Maßnahmenfensters angezeigt. Durch Klicken auf ein Maßnahmenregister werden alle verfügbaren Benutzeroptionen in einer Liste von Unterkategorien angezeigt.

Wenn Sie auf ein Objekt in der System-/Servermodulstruktur klicken, wird das Maßnahmenfenster dieses Objekts geöffnet und die verfügbaren Maßnahmenregister werden angezeigt. Der Datenbereich geht standardmäßig zu einer vorbestimmten Unterkategorie des ersten Maßnahmenregisters für das ausgewählte Objekt.

Die vorbestimmte Unterkategorie ist gewöhnlich die erste Option. So wird z. B. durch Klicken auf das Objekt **Hauptsystemgehäuse/Hauptsystem** ein Maßnahmenfenster geöffnet, in dem das Maßnahmenregister **Eigenschaften** mit der Unterkategorie **Funktionszustand** im Datenbereich des Fensters angezeigt wird.

Datenbereich

Der Datenbereich befindet sich unter den Maßnahmenregistern auf der rechten Seite der Startseite. Im Datenbereich werden Tasks ausgeführt oder Details zu Systemkomponenten angezeigt. Der Inhalt des Fensters hängt von dem System Baumobjekt und Handeln Registerkarte, die derzeit ausgewählt ist. Wenn Sie z. B. **BIOS** in der Systemstruktur wählen, wird automatisch das Register **Eigenschaften** ausgewählt und die Versionsinformationen für die System-BIOS erscheinen im Datenbereich. Der Datenbereich des Maßnahmenfensters enthält viele allgemeine Funktionen, einschließlich Statusanzeigen, Task-Schaltflächen, unterstrichene Einträge und Messanzeigen.

Die Benutzeroberfläche von Server Administrator zeigt das Datum im Format <MM/TT/JJJJ> an.

System/Servermodul-Komponentenstatusanzeigen

Die Symbole neben den Komponentennamen zeigen den Status der jeweiligen Komponenten an (seit der letzten Seitenaktualisierung).

Tabelle 8. System/Servermodul-Komponentenstatusanzeigen

Beschreibung	Symbol
	Die Komponente ist funktionsfähig (normal).
	Die Komponente weist eine Warnung (ein nicht-kritisches Problem) auf. Ein Warnzustand tritt ein, wenn eine Sonde oder ein anderes Überwachungsmittel einen Wert für eine Komponente ermittelt, der zwischen bestimmte Minimal- und Maximalwerte fällt. Ein Warnzustand erfordert sofortige Aufmerksamkeit.
	Komponente ist ausgefallen oder befindet sich in einem kritischen Zustand. Ein kritischer Zustand tritt ein, wenn eine Sonde oder ein anderes Überwachungsmittel einen Wert für eine Komponente ermittelt, der zwischen bestimmte Minimal- und Maximalwerte fällt. Ein kritischer Zustand erfordert sofortige Aufmerksamkeit.
	Der Funktionszustand der Komponente ist unbekannt.

Task-Schaltflächen

Die meisten auf der Server Administrator-Startseite auftretenden Fenster enthalten mindestens fünf Task-Schaltflächen: **Drucken**, **Exportieren**, **E-Mail**, **Hilfe** und **Aktualisieren**. In bestimmten Server Administrator-Fenstern gibt es weitere Task-Schaltflächen. Zum Beispiel enthält das Fenster **Protokoll** auch die Task-Schaltflächen **Speichern unter** und **Protokoll löschen**.

- Durch Klicken auf **Drucken** ( ) druckt eine Kopie des offenen Fensters auf dem Standarddrucker aus.
- Durch Klicken auf **Exportieren** ( ) wird eine Textdatei erstellt, in der die Werte jedes Datenfeldes in dem geöffneten Fenster aufgelistet sind. Die Exportdatei wird an dem von Ihnen bestimmten Speicherort gespeichert. Unter „Einstellung der Benutzer" und „Systemeinstellungen" finden Sie Informationen zum Anpassen von Begrenzungszeichen, mit denen die Datenfeldwerte getrennt werden.
- Durch Klicken auf **E-Mail** ( ) wird eine an den vorbestimmten E-Mail-Empfänger adressierte E-Mail-Meldung erstellt. Unter „Einstellung der Benutzer" und „Systemeinstellungen" finden Sie eine Anleitung zur Einrichtung Ihres E-Mail-Servers und des Standard-E-Mail-Empfängers.
- Durch Klicken auf **Aktualisieren** ( ) werden Statusinformationen über Systemkomponenten in den Datenbereich des Maßnahmenfensters geladen.
- Durch Klicken auf **Speichern unter** wird eine HTML-Datei des Maßnahmenfensters in einer **.zip**-Datei gespeichert.
- Durch Klicken auf **Protokoll löschen** werden alle Ereignisse aus dem im Datenbereich des Maßnahmenfensters angezeigten Protokoll gelöscht.

- Durch Klicken auf **Hilfe** () werden weitere Einzelheiten über das bestimmte Fenster oder die betrachtete Task-Schaltfläche bereitgestellt.

ANMERKUNG: Die Schaltflächen **Exportieren**, **E-Mail** und **Speichern unter** werden nur für Benutzer angezeigt, die mit Hauptbenutzer- oder Administrator-Rechten angemeldet sind. Die Schaltfläche **Protokoll löschen** wird nur für Benutzer angezeigt, die mit Administrator-Rechten angemeldet sind.

Unterstrichene Einträge

Durch Klicken auf einen unterstrichenen Eintrag im Datenbereich des Maßnahmenfensters werden weiterführende Details über den Eintrag angezeigt.

Messanzeigen

Temperatursonden, Lüftersonden und Spannungssonden werden jeweils durch eine Messanzeige dargestellt. Die folgende Abbildung zeigt z. B. Messwerte von der CPU-Lüftersonde eines Systems.

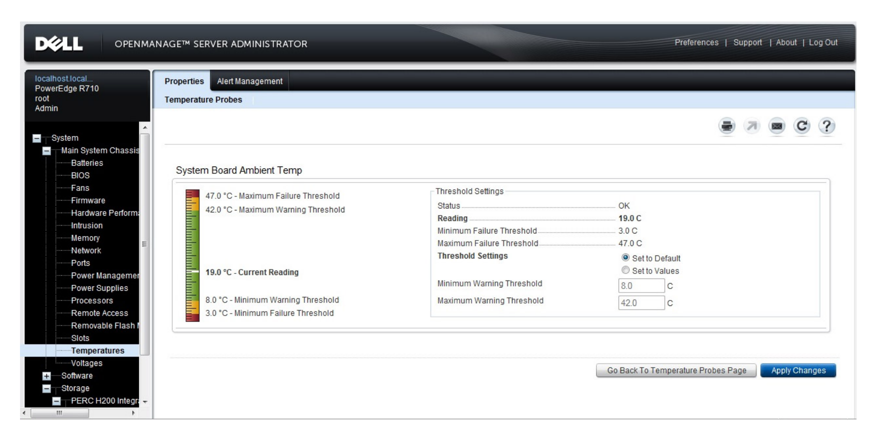


Abbildung 3. Messanzeige

Online-Hilfe verwenden

Kontextbezogene Online-Hilfe ist verfügbar für jedes Fenster der Startseite von Server Administrator. Durch Klicken auf **Hilfe** auf der allgemeinen Navigationsleiste wird ein unabhängiges Hilfefenster geöffnet, das detaillierte Informationen über das betrachtete Fenster enthält. Die Onlinehilfe ist darauf ausgelegt, Sie durch die spezifischen Maßnahmen zu leiten, die zur Ausführung aller Aspekte des Server Administrator-Dienstes erforderlich sind. Online-Hilfe ist verfügbar für alle Fenster, die angezeigt werden können, basierend auf den Software- und Hardwaregruppen, die der Server Administrator auf dem System feststellt, und der Benutzerberechtigungsebene.

Einstellungen-Startseite verwenden

Im linken Fenster der Startseite Einstellungen (wo auf der Server Administrator-Startseite die Systemstruktur angezeigt wird) werden alle verfügbaren Konfigurationsoptionen im Systemstrukturfenster angezeigt.

Die verfügbaren Konfigurationsoptionen der Einstellungen-Startseite sind:

- Allgemeine Einstellungen

- Server Administrator

Sie können das Register **Einstellungen** einsehen, nachdem Sie sich zur Verwaltung eines Remote-Systems angemeldet haben. Dieses Register ist auch verfügbar, wenn Sie sich zur Verwaltung des Server Administrator Web Servers oder des lokalen Systems anmelden.

Wie die Server Administrator-Startseite besteht auch die **Einstellungen**-Startseite aus drei Hauptbereichen:

- Die Allgemeine Navigationsleiste stellt Verknüpfungen zu allgemeinen Diensten zur Verfügung.
  - Klicken Sie auf **Startseite**, um zur Server Administrator-Startseite zurückzukehren.
- Im linken Fenster der Startseite **Einstellungen** (wo auf der Server Administrator-Startseite die Systemstruktur angezeigt wird) werden die Einstellungskategorien für das verwaltete System angezeigt.
- Im Maßnahmenfenster werden die verfügbaren Einstellungen und vorbestimmten Einstellungen für das verwaltete System oder den Server Administrator Web Server angezeigt.

Managed System-Einstellungen

Wenn Sie sich bei einem Remote-System anmelden, befindet sich die Einstellungen-Startseite standardmäßig im **Knotenkonfiguration**sfenster im Register **Einstellungen**.

Klicken Sie auf das Objekt Server Administrator, um Benutzern den Zugriff als Benutzer oder Hauptbenutzer zu gewähren bzw. zu verweigern. Abhängig von den Benutzergruppen-Berechtigungen kann das Maßnahmenfenster des Server Administrator-Objekts die Registerkarte **Einstellungen** aufweisen oder nicht.

Im Register **Einstellungen** können Sie Folgendes durchführen:

- Zugriff von Benutzern mit Benutzer- oder Hauptbenutzerrechten aktivieren oder deaktivieren
- Wählen Sie das Format der Warnungsmeldungen aus

  ANMERKUNG: Mögliche Formate sind **klassisch** und **erweitert**. Das Standardformat ist **klassisch**, welches das Legacy-Format ist.
- Die Befehlsprotokollgröße konfigurieren
- SNMP konfigurieren

Server Administrator Web Server-Einstellungen

Wenn Sie sich zur Verwaltung des Server Administrator Web Servers anmelden, befindet sich die **Einstellungen-**Startseite standardmäßig im Fenster Benutzereinstellungen im Register Einstellungen.

Aufgrund der Trennung des Server Administrator Web Servers vom verwalteten System werden die folgenden Optionen angezeigt, wenn Sie sich unter Verwendung des Manage Web Server-Links bei Server Administrator Web Server anmelden:

- Web Server-Einstellungen
- X.509-Zertifikatsverwaltung

Weitere Informationen zum Zugriff auf diese Funktionen finden Sie unter Server Administrator Services - Übersicht.

Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup

Benutzer- und Systemeinstellungen vornehmen

Die Einstellungen für Benutzer und sicheren Port-Systemeinstellungen werden von der **Einstellungen**-Startseite eingestellt.



ANMERKUNG: Zum Festlegen oder Zurücksetzen von Benutzer- oder Systemeinstellungen müssen Sie mit Administrator-Rechten angemeldet sein.

Richten Sie Ihre Benutzereinstellungen ein:

1. Klicken Sie auf **Einstellungen** auf der allgemeinen Navigationsleiste.

   Es wird die Startseite **Einstellungen** angezeigt.
2. Klicken Sie auf **Allgemeine Einstellungen**.
3. Um einen vorbestimmten E-Mail-Empfänger hinzuzufügen, geben Sie die E-Mail-Adresse des festgelegten Dienstkontakts im Feld **Senden an**: ein und klicken Sie auf **Übernehmen**.

   ANMERKUNG: Durch Klicken auf **E-Mail** ( ) in einem beliebigen Fenster wird eine E-Mail-Nachricht, an die eine HTML-Datei des Fensters angehängt ist, an die vorgegebene E-Mail-Adresse gesendet.

   ANMERKUNG: Die Webserver-URL wird nicht bewahrt, wenn Sie den Server Administrator-Dienst oder das System, auf dem Server Administrator installiert ist, neu starten. Verwenden Sie den Befehl **omconfig**, um die URL neu einzugeben.

Secure Port-System

Führen Sie folgende Schritte durch, um die Secure Port-Systemeinstellungen festzulegen.

1. Klicken Sie auf **Einstellungen** auf der allgemeinen Navigationsleiste.

   Die **Einstellungen**-Startseite wird eingeblendet.
2. Klicken Sie auf **Allgemeine Einstellungen**.
3. Im Fenster **Servereinstellungen** stellen Sie die Optionen nach den Erfordernissen ein.
   - Die Funktion **Sitzungszeitüberschreitung (Minuten)** kann dazu verwendet werden, eine Grenze für die Zeitdauer die eine Server Administrator-Sitzung aktiv bleiben kann, zu setzen. Wählen Sie **Aktivieren** aus, um den Server Administrator die Sitzung beenden zu lassen, wenn während eines festgelegten Zeitraums von Minuten keine Benutzermaßnahme stattfindet. Benutzer, deren Sitzung beendet wird, müssen sich erneut anmelden. Wählen Sie **Deaktivieren**, um die Funktion **Sitzungszeitüberschreitung (Minuten)** von Server Administrator zu deaktivieren.
   - Das Feld **HTTPS-Schnittstelle** bestimmt die sichere Schnittstelle für den Server Administrator. Die sichere Standardschnittstelle für Server Administrator ist 1311.

     ANMERKUNG: Die Änderung der Anschlussnummer auf eine ungültige bzw. eine bereits belegte Anschlussnummer kann andere Anwendungen oder Browser beim Zugriff auf den Server Administrator auf dem verwalteten System behindern. Eine Liste der Standardschnittstellen finden Sie im *Server Administrator Installation Guide* (Server Administrator-Installationshandbuch) unter **dell.com/openmanagemanuals**.
   - Das Feld **Zu bindende IP-Adresse** legt die IP-Adresse(n) für das Managed System fest, mit der sich der Server Administrator zu Beginn einer Sitzung verbindet. Wählen Sie **Alle** aus, um an alle für

das System in Frage kommenden IP-Adressen zu binden. Wählen Sie **Spezifisch** aus, um an eine spezifische IP-Adresse zu binden.

 ANMERKUNG: Wenn der Wert für **IP-Adresse binden an** auf einen anderen Wert als **Alle** geändert wird, dann kann dies dazu führen, dass andere Anwendungen oder Browser nicht mehr auf den Server Administrator im verwalteten System zugreifen können.

- Aus dem Feld **Senden an** gehen die E-Mail-Adressen hervor, an die standardmäßig E-Mails zu Aktualisierungen gesendet werden. Sie können mehrere E-Mail-Adressen konfigurieren und ein Komma zum Abtrennen der einzelnen E-Mail-IDs verwenden.
- Die Felder **SMTP-Servername (oder die IP-Adresse)** und **DNS-Suffix für SMTP-Server** bestimmen das Suffix für das Einfache Mail-Übertragungsprotokoll (SMTP) und den Domänennamenserver (DNS) einer Firma oder Organisation. Um für Server Administrator das Versenden von E-Mails zu aktivieren, muss die IP-Adresse und das DNS-Suffix für den SMTP-Server für die Firma oder Organisation in die entsprechenden Felder eingeben werden.

  ANMERKUNG: Aus Sicherheitsgründen gestattet Ihre Firma eventuell nicht, dass E-Mails über den SMTP-Server an externe Empfänger gesendet werden.

- Im Feld **Befehlsprotokollumfang** wird die maximale Dateigröße in MB für die Befehlsprotokolldatei festgelegt.

  ANMERKUNG: Dieses Feld wird nur angezeigt, wenn Sie sich zur Verwaltung des Server Administrator Web Servers anmelden.

- Das Feld **Support-Verknüpfung** enthält die URL für die Unternehmenseinheit, die die Unterstützung für das verwaltete System leistet.
- Das Feld **Benutzerdefinierte Begrenzungszeichen** bestimmt das Zeichen, das zur Trennung der Datenfelder der Dateien verwendet wird, die durch die Schaltfläche **Exportieren** erstellt werden. Das Zeichen **;** ist das standardmäßige Begrenzungszeichen. Weitere Optionen sind **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **|** und **,**.
- Das Feld **SSL-Verschlüsselung** gibt die Verschlüsselungsstufen für die gesicherten HTTPS-Sitzungen an. Zu den verfügbaren Verschlüsselungsstufen gehören **Automatische Verhandlung** und **128 Bit oder höher**.

  - **Automatische Verhandlung** – Ermöglicht die Verbindung über Browser mit beliebiger Verschlüsselungsstärke. Der Browser verhandelt automatisch mit dem Server Administrator Web Server und verwendet die höchste verfügbare Verschlüsselungsstufe für die Sitzung. Frühere Browser mit schwächerer Verschlüsselung können sich auch mit dem Server Administrator verbinden.
  - **128-Bit oder höher** – Ermöglicht Verbindungen über Browser mit 128-Bit- oder höherer Verschlüsselungsstärke. Eine der folgenden Verschlüsselungssammlungen ist basierend auf dem Browser für beliebige feststehende Sitzungen anwendbar:

```
SSL_RSA_WITH_RC4_128_SHA

SSL_RSA_WITH_RC4_128_MD5

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA
```

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

 ANMERKUNG: Die Option **128 Bit oder höher** lässt keine Verbindungen von Browsern mit niedrigeren SSL-Verschlüsselungsstärken zu, wie z. B. 40 Bit und 56 Bit.

 ANMERKUNG: Wenn die Verschlüsselungsstufe auf **128 Bit oder höher** eingestellt ist, können Sie mit einem Browser mit denselben oder höheren Verschlüsselungsstufen auf die Server Administrator-Einstellungen zugreifen oder diese ändern.

- **Schlüsselsignierungsalgorithmus (Für Selbstsignierungszertifikat)** – Erlaubt Ihnen, einen unterstützten Signierungsalgorithmus auszuwählen. Wenn Sie **SHA 512** oder **SHA 256** auswählen, müssen Sie sicherstellen, dass Ihr Betriebssystem/Browser diesen Algorithmus unterstützt. Wenn Sie eine dieser Optionen auswählen, ohne dass die erforderliche Betriebssystem-/Browserunterstützung zur Verfügung steht, zeigt Server Administrator den Fehler `cannot display the webpage`. Dieses Feld bezieht sich ausschließlich auf von Server Administrator automatisch erstellte, selbst unterzeichnete Zertifikate. Die Drop-Down-Liste wird grau unterlegt, wenn Sie neue Zertifikate in Server Administrator importieren oder erstellen.
- **Java Runtime Environment** – Erlaubt Ihnen, eine der folgenden Optionen auszuwählen:
  - **Gebündelte JRE** – Aktiviert die Verwendung des, zusammen mit System Administrator bereitgestelltem, JRE.
  - **System-JRE** – Aktiviert die Verwendung des auf dem System installiertem JRE. Wählen Sie die erforderliche Version aus der Dropdown-Liste aus.

   ANMERKUNG: Wenn das JRE auf dem System, auf dem Server Administrator läuft, nicht existiert, wird das JRE, das mit Server Administrator bereitgestellt wurde, verwendet.

4. Wenn Sie alle Einstellungen im Fenster **Servereinstellungen** vorgenommen haben, klicken Sie auf **Änderungen anwenden**.

    ANMERKUNG: Starten Sie den Server Administrator Web Server erneut, um die Änderungen wirksam zu machen.

X.509-Zertifikatsverwaltung

ANMERKUNG: Für die Zertifikatsverwaltung müssen Sie mit Administrator-Zugriffsrechten angemeldet sein.

Web-Zertifikate sind erforderlich zum Schutz der Identität eines Remote-Systems und damit sichergestellt werden kann, dass die mit dem Remote-System ausgetauschten Informationen von anderen Parteien weder gesehen noch geändert werden. Um die Systemsicherheit zu gewährleisten, wird Folgendes dringend empfohlen:

- Entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes X.509-Zertifikat wiederzuverwenden oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) zu importieren.
- Alle Systeme, auf denen Server Administrator installiert ist, haben eindeutige Host-Namen.

Um X.509-Zertifikate über die **Einstellungen**-Startseite zu verwalten, klicken Sie auf **Allgemeine Einstellungen**, dann auf das Register **Web Server** und auf **X.509-Zertifikat**.

Die folgenden Optionen sind verfügbar:

- **Ein neues Zertifikat erstellen** – Erstellt ein neues selbstsigniertes Zertifikat, das für die SSL-Kommunikation zwischen dem Server, auf dem Server Administrator ausgeführt wird, und dem Browser verwendet wird.



ANMERKUNG: Wenn ein selbstsigniertes Zertifikat verwendet wird, erstellen die meisten Webbrowser eine *nicht vertrauenswürdige* Warnung, wenn dieses Zertifikat von einer vom Betriebssystem genehmigten Zertifizierungsstelle (CA) nicht signiert wurde. Einige sichere Browser-Einstellungen können auch die selbstsignierten SSL-Zertifikate blockieren. Die OMSA-Web-GUI erfordert ein CA-signiertes Zertifikat für solche sichere Browser.

- **Zertifikat-Pflege** – Hier können Sie eine Zertifikatsignierungsanforderung (CSR) erstellen, die alle Zertifikatinformationen über den Host enthält, die von der CA erfordert werden, um die Erstellung eines vertrauenswürdigen Web-Zertifikats zu automatisieren. Sie können die erforderliche CSR-Datei entweder von den Anleitungen auf der Seite „Zertifikatssignierungsanforderung (CSR)" abrufen, oder Sie können den gesamten Text im Textfeld auf der CSR-Seite kopieren und ihn dann in das Zertifikatsformular zum Einsenden einfügen. Der Text muss das Base64-kodierte Format aufweisen.



ANMERKUNG: Als Option steht Ihnen auch zur Verfügung, die Zertifikatinformationen anzuzeigen und das Zertifikat zu exportieren, das beim Base–64-Format, das von anderen Webservices importiert werden kann, verwendet wird.

- **Zertifikatskette importieren** – Mit dieser Option können Sie die von einer vertrauenswürdigen Zertifizierungsstelle (CA) signierte Zertifikatskette (im Format PKCS # 7) importieren. Das Zertifikat kann im DER- oder Base64-kodiertem Format sein.

Server Administrator Web Server-Maßnahmenregister

Im Folgenden werden die Aktionsregisterkarten aufgelistet, die angezeigt werden, wenn Sie sich zum Verwalten des Server Administrator-Webservers anmelden:

- Eigenschaften
- Herunterfahren
- Protokolle
- Warnungsverwaltung
- Sitzungsverwaltung

Server Administrator-Befehlszeilenschnittstelle verwenden

Die Befehlszeilenschnittstelle von Server Administrator (CLI) ermöglicht es Benutzern, wichtige Systemverwaltungs-Tasks von der Befehlseingabeaufforderung des Betriebssystems eines überwachten Systems auszuführen.

In vielen Fällen lässt die CLI Benutzer mit gut definierten Aufgaben Informationen über das System schnell abrufen. Mit CLI-Befehlen können Administratoren beispielsweise Stapelverarbeitungsprogramme oder Skripts schreiben, die zu bestimmten Zeiten ausgeführt werden. Wenn diese Programme ausgeführt werden, können sie Berichte über wichtige Komponenten, z. B. Lüftergeschwindigkeit, sammeln. Mit zusätzlichem Skripting kann die CLI zur Sammlung von Daten während Spitzenbelastungszeiten verwendet werden, die dann mit den zu Zeiten geringerer Systembelastung gesammelten Daten verglichen werden. Befehlsergebnisse können zur späteren Analyse an eine Datei weitergeleitet werden. Die Berichte können Administratoren bei der Sammlung von Informationen helfen, die zur Feststellung von Gebrauchsmustern, zur Rechtfertigung des Einkaufs neuer Systemressourcen oder zur Konzentration auf den Zustand einer Problemkomponente verwendet werden können.

Vollständige Anleitungen über die Funktionen und Verwendung der CLI finden Sie im *Server Administrator Command Line Interface Guide* (Benutzerhandbuch für die Server Administrator-Befehlszeilenschnittstelle) unter **dell.com/openmanagemanuals**.

4

Server Administrator-Dienste

Der Server Administrator-Instrumentierungsdienst überwacht den Funktionszustand eines Systems und gewährt schnellen Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von marktüblichen Systemverwaltungsagenten gesammelt werden. Die Berichts- und Ansichtsfunktionen ermöglichen den Abruf des Gesamtfunktionszustands für alle Gehäuse, die das System ausmachen. Auf der Subsystemebene kann man Informationen über Spannungen, Temperaturen, Lüftergeschwindigkeiten und Speicherfunktionen an den wichtigsten Punkten des Systems anzeigen. Eine detaillierte Beschreibung aller Einzelheiten zu den relevanten Betriebskosten (COO) des Systems ist in einer Zusammenfassung verfügbar. Die Versionsinformationen für BIOS, Firmware, Betriebssystem und alle installierte System Management Software können einfach abgerufen werden.

Ferner können Systemadministratoren den Instrumentierungsdienst zur Ausführung der folgenden wesentlichen Tasks verwenden:

- Festlegung der Minimal- und Maximalwerte für bestimmte kritische Komponenten. Diese Werte, Schwellenwerte genannt, bestimmen den Bereich, in dem ein Warnungsereignis für die betreffende Komponente auftritt (Minimal- und Maximalausfallwerte werden vom Hersteller des Systems festgelegt).
- Festlegung der Systemreaktion bei Auftreten eines Warnungs- oder Ausfallereignisses. Benutzer können die Maßnahmen konfigurieren, die ein System als Reaktion auf Benachrichtigungen über Warnungs- und Ausfallereignisse ergreift. Andererseits können Benutzer, die über Rund-um-die-Uhr-Überwachung verfügen, festlegen, dass keine Maßnahmen zu ergreifen sind, und sich auf das menschliche Urteil über die beste Reaktion auf ein Ereignis verlassen.
- Bestücken aller der benutzerfestlegbaren Werte für das System, z. B. Systemname, Telefonnummer des primären Systembenutzers, Abschreibungsmethode, ob das System gemietet oder gekauft ist, usw.

Systemverwaltung

Die Startseite von Server Administrator wird automatisch auf der Ansicht des Systemobjekts der Systemstrukturansicht geöffnet. Standardeinstellung für das **System**objekt öffnet die **Zustands**komponenten im Register **Eigenschaften**.

Standardmäßig öffnet die Startseite **Einstellungen** die **Knotenkonfiguration**.

Auf der Startseite **Einstellungen** können Sie den Zugriff auf Benutzer mit Benutzer- und Hauptbenutzer-Berechtigungen einschränken, das SNMP-Kennwort festlegen und Benutzer- und SM SA-Verbindungsdienst-Einstellungen konfigurieren.

ANMERKUNG: Kontextbezogene Online-Hilfe ist verfügbar für jedes Fenster der Startseite von Server Administrator. Klicken Sie auf **Hilfe** ( ) um ein unabhängiges Hilfefenster zu öffnen, das detaillierte Informationen über das betrachtete Fenster enthält. Die Onlinehilfe ist darauf ausgelegt, Sie durch die spezifischen Maßnahmen zu leiten, die zur Ausführung aller Aspekte des Server Administrator-Dienstes erforderlich sind. Online-Hilfe ist verfügbar für alle Fenster, die angezeigt werden können, basierend auf den Software- und Hardwaregruppen, die der Server Administrator auf dem System feststellt, und der Benutzerberechtigungsebene.



ANMERKUNG: Admin- oder Hauptbenutzer-Berechtigungen sind zur Ansicht vieler der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Zugriffsrechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren**.

System-/Servermodul-Strukturobjekte verwalten

Die Systemstruktur von Server Administrator zeigt alle sichtbaren Systemobjekte basierend auf den Software- und Hardwaregruppen an, die Server Administrator auf dem verwalteten System feststellt, und auf den Zugriffsrechten des Benutzers. Die Systemkomponenten sind nach Komponententyp kategorisiert. Wenn Sie das Hauptobjekt – **Modulares Gehäuse** – **System/Servermodul** – expandieren, sind die System-komponenten-Hauptkategorien, die erscheinen können, **Hauptsystemgehäuse/Hauptsystem**, **Software** und **Speicher**.

Wenn der Storage Management-Dienst installiert ist, erweitert sich das Speicherstrukturobjekt abhängig vom Controller und Speicher, die am System angeschlossen sind, um verschiedene Objekte anzuzeigen.

Detaillierte Informationen zur Storage Management-Dienst-Komponente finden Sie im *Storage Management User's Guide* (Benutzerhandbuch zu Storage Management) unter **dell.com/openmanagemanuals**.

Server Administrator-Startseite-Systemstrukturobjekte

In diesem Abschnitt finden Sie Informationen über die Objekte in der Systemstruktur auf der Server Administrator-Startseite. Aufgrund der Einschränkungen der ESXi Version 5.X-Betriebssysteme sind einige der vormals verfügbaren Funktionen von Server Administrator in dieser Version nicht mehr verfügbar.

Die nicht unterstützten Funktionen unter ESXi 5.X sind:

- Informationen zur FCoE-Fähigkeit und zur iSoE-Fähigkeit
- Warnungsverwaltung – Warnungsmaßnahmen
- Netzwerkschnittstelle – Administrativer Status, DMA, IP-Adresse,
- Netzwerkschnittstelle – Betriebsstatus
- Remote-Herunterfahren – Ein-/Ausschalten mit vorherigem Herunterfahren des Betriebssystems
- Info-Details – Details zu den Server Administrator-Komponenten, die nicht auf der Registerkarte **Details** aufgeführt sind
- Rolemap



ANMERKUNG: Server Administrator zeigt das Datum stets im Format *<MM/TT/JJJJ>* an.

ANMERKUNG: Admin- oder Hauptbenutzer-Berechtigungen sind zur Ansicht vieler der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Zugriffsrechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren**.

Modulares Gehäuse



ANMERKUNG: Für die Zwecke von Server Administrator bezieht sich der Begriff „modulares Gehäuse" auf ein System, das möglicherweise ein oder mehrere modulare Systeme enthält, die in der Systemstruktur als separate Servermodule angezeigt werden. Ebenso wie ein selbstständiges Servermodul enthält ein modulares Gehäuse alle wichtigen Komponenten eines Systems. Der einzige Unterschied besteht darin, dass Steckplätze für mindestens zwei Servermodule innerhalb eines größeren Containers vorhanden sind, von denen jeder ein ebenso vollständiges System ist, wie ein Servermodul.

Um die Gehäuseinformationen des modularen Systems und die CMC-Informationen (Chassis Management Controller) anzuzeigen, klicken Sie auf das Objekt **Modulares Gehäuse**.

- **Registerkarte: Eigenschaften**
- **Unterregister: Informationen**

Im Register Eigenschaften können Sie Folgendes durchführen:

- Die Gehäuseinformationen für das modulare System anzeigen, das überwacht wird.
- Detaillierte Chassis Management Controller (CMC)-Informationen für das modulare System anzeigen, das überwacht wird.

Chassis Management Controller (CMC) aufrufen und verwenden

So rufen Sie das Fenster **Anmelden** des Geräteverwaltungs-Controllers (CMC) über die Startseite von Server Administrator auf:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**.
2. Klicken Sie auf das Register **CMC-Informationen** und dann auf **CMC-Web-Schnittstelle starten**. Das CMC-**Anmelde**fenster wird eingeblendet.

Sie können Ihr modulares Gehäuse nach dem Herstellen einer Verbindung zum CMC überwachen und verwalten.

System-/Servermodul Eigenschaften

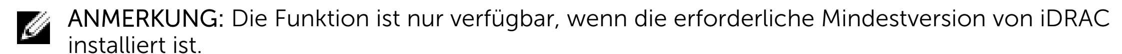
Das Objekt **System/Servermodul** enthält drei Hauptsystemkomponentengruppen: Hauptsystemgehäuse/Hauptsystem, Software und Speicher. Die Startseite von Server Administrator wird automatisch auf der Ansicht des **System**objekts der Systemstrukturansicht geöffnet. Die meisten Verwaltungsfunktionen können vom Maßnahmenfenster des Objekts **System-/Servermodul** getätigt werden. Das Maßnahmenfenster des Objekts **System-/Servermodul** weist abhängig von den Berechtigungen der Benutzergruppe folgende Register auf: **Lizenzierung**, **Eigenschaften**, **Herunterfahren**, **Protokolle**, **Warnungsverwaltung** und **Sitzungsverwaltung**.

Lizenzierung

Unterregister: Informationen | Lizenzierung

Im Unterregister Lizenzierung können Sie:

- Einstellungen für die Verwaltung von Integrated Dell Remote Access Controller (iDRAC) zum Importieren, Exportieren, Löschen oder zum Austauschen der digitalen Lizenz der Hardware festlegen.
- Die Details der Geräte anzeigen. Diese Details schließen den Lizenzierungsstatus, die Beschreibung der Lizenz, Berechtigungs-ID und Ablaufdatum der Lizenz ein.



ANMERKUNG: Die Funktion ist nur verfügbar, wenn die erforderliche Mindestversion von iDRAC installiert ist.

Eigenschaften

Unterregister: Funktionszustand | Zusammenfassung | Bestandsinformationen | Autom. Wiederherstellung

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- Den aktuellen Warnungsfunktionszustand für Hardware- und Softwarekomponenten im Objekt **Hauptsystemgehäuse/Hauptsystem** und das **Speicher**-Objekt anzeigen.
- Die detaillierten Zusammenfassungen für alle Komponenten im überwachten System anzeigen.
- Die Bestandsinformationen für das überwachte System anzeigen und konfigurieren.
- Die automatischen Systemwiederherstellungsmaßnahmen (Betriebssystem-Watchdog-Zeitgeber) für das überwachte System anzeigen und einstellen.

ANMERKUNG: Automatische Systemwiederherstellungsoptionen sind möglicherweise nicht verfügbar, wenn der Watchdog-Zeitgeber des Betriebssystems in BIOS aktiviert ist. Der Watchdog-Zeitgeber des Betriebssystems muss deaktiviert sein, damit die Optionen der automatischen Wiederherstellung konfiguriert werden können.

ANMERKUNG: Automatische Systemwiederherstellungsmaßnahmen werden eventuell nicht genau nach eingestellter Zeitüberschreitungsperiode (in Sekunden) ausgeführt, wenn der Watchdog ein System identifiziert, das nicht antwortet. Der Maßnahmen-Ausführungszeitraum erstreckt sich von n-h+1 bis n+1 Sekunden, wobei n die Zeitüberschreitungsperiode ist und h das Heartbeat-Intervall. Der Wert des Heartbeat-Intervalls beträgt 7 Sekunden, wenn n <= 30 ist, und 15 Sekunden, wenn n > 30 ist.

ANMERKUNG: Die Funktionalität der Watchdog-Zeitgeberfunktion kann in einem Fall, in dem ein nicht behebbares Speicherereignis im System DRAM Bank_1 auftritt, nicht garantiert werden. Wenn an diesem Ort ein nicht behebbares Speicherereignis auftritt, ist es möglich, dass der BIOS-Code-Resident an dieser Stelle beschädigt wird. Da die Watchdog-Funktion einen Aufruf zu BIOS verwendet, um das Herunterfahren- oder Neustartverhalten zu beeinflussen, funktioniert die Funktion eventuell nicht richtig. Wenn dies eintritt, müssen Sie das System manuell neu starten. Der Watchdog-Zeitgeber kann maximal auf 720 Sekunden eingestellt werden.

Herunterfahren

Unterregister: Remote-Herunterfahren | Temperaturbedingtes Herunterfahren | Web Server herunterfahren

Im Register **Herunterfahren** können Sie Folgendes durchführen:

- Die Optionen zum Herunterfahren und Remote-Herunterfahren des Betriebssystems konfigurieren
- Die Schweregradstufe des temperaturbedingten Herunterfahrens einstellen, das das System herunterfährt, wenn ein Temperatursensor eine Warnung oder einen Fehlerwert zurückgibt.

 ANMERKUNG: Ein temperaturbedingtes Herunterfahren erfolgt nur dann, wenn die vom Sensor gemeldete Temperatur über dem Temperaturschwellenwert liegt. Ein temperaturbedingtes Herunterfahren erfolgt nicht, wenn die vom Sensor gemeldete Temperatur unter dem Temperaturschwellenwert liegt.

- Fahren Sie den DSM SA-Verbindungsdienst (Web Server) herunter.

 ANMERKUNG: Server Administrator ist nach wie vor verfügbar und verwendet die Befehlszeilenoberfläche (CLI), wenn der DSM SA-Verbindungsdienst heruntergefahren ist. Die CLI-Funktionen erfordern nicht, dass der DSM SA-Verbindungsdienst ausgeführt wird.

Protokolle

Unterregister: Hardware | Warnung | Befehl

Im Register **Protokolle** können Sie Folgendes durchführen:

- Das Protokoll für die integrierte Systemverwaltung (ESM) oder das Systemereignisprotokoll (SEL) als Liste aller mit den Hardwarekomponenten des Systems verbundenen Ereignissen anzeigen. Das Statusanzeigesymbol neben dem Protokollnamen wechselt vom normalen Status) zum nicht-kritischen Status () wenn die Protokolldatei 80 Prozent der Kapazität erreicht.

 ANMERKUNG: Sie sollten das Hardwareprotokoll löschen, wenn es 80 Prozent der Kapazität erreicht. Wenn dem Protokoll erlaubt wird, 100 Prozent der Kapazität zu erreichen, werden die neuesten Ereignisse aus dem Protokoll entfernt und verworfen.

- Das Warnungsprotokoll auf einer Liste aller vom Server Administrator-Instrumentierungsdienst in Reaktion auf Sensorstatusänderungen erzeugten Ereignissen und anderer überwachter Parameter anzeigen.

 ANMERKUNG: Weitere Informationen über die Beschreibung, den Schweregrad und die Ursache aller Warnungsereignis-IDs finden Sie im *Server Administrator Messages Reference Guide* (Dell OpenManage Server Administrator-Meldungs-Referenzhandbuch) unter dell.com/openmanagemanuals.

- Zeigen Sie das Befehlsprotokoll für eine Liste mit jedem von der **Server Administrator**-Startseite oder der Befehlszeilenoberfläche ausgeführten Befehl an.

 ANMERKUNG: Informationen zum Anzeigen, Drucken, Speichern und Senden von Protokollen per E-Mail finden Sie unter „Server Administrator-Protokolle".

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | Plattformereignisse | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemkomponentensensor einen Warnungs- oder Ausfallwert sendet.
- Die aktuellen Plattformereignisfilter-Einstellungen anzeigen und die Plattformereignisfilter-Maßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemkomponentensensor einen Warnungs- oder Ausfallwert sendet. Sie können auch über die Option **Ziel konfigurieren** ein Ziel auswählen (IPv4- oder IPv6-Adresse), an das eine Warnung über ein Plattformereignis gesendet werden soll.

 ANMERKUNG: Server Administrator zeigt die Scope-ID der IPv6-Adresse nicht in seiner grafischen Benutzeroberfläche an.

- Prüfen Sie die derzeitigen SNMP-Trap-Warnungsschwellenwerte und setzen Sie die Warnungsschwellenwerte für instrumentierte Systemkomponenten. Die ausgewählten Traps werden

ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

 ANMERKUNG: Im Fenster **Warnungsmaßnahmen** sind alle Warnungsmaßnahmen für alle potenziellen Systemkomponentensensoren aufgelistet, auch wenn diese in Ihrem System nicht vorhanden sind. Das Setzen von Warnungsmaßnahmen für Systemkomponentensensoren, die auf dem System nicht vorhanden sind, hat keine Auswirkungen.

 ANMERKUNG: Auf einem beliebigen Microsoft Windows-Betriebssystem muss die Option **Erweiterte Systemeinstellungen** → **Erweiterte Wiederherstellung** im Betriebssystem deaktiviert werden, um sicherzustellen, dass Server Administrator Automatische Systemwiederherstellungswarnungen erstellt werden.

Sitzungsverwaltung

Unterregister: Sitzung

Im Register **Sitzungsverwaltung** können Sie Folgendes durchführen:

- Sitzungsinformationen für die aktuellen Benutzer anzeigen, die sich bei Server Administrator angemeldet haben.
- Benutzersitzungen beenden.

 ANMERKUNG: Nur Benutzer mit Administratorberechtigungen können die **Sitzungsverwaltung**sseite anzeigen und Sitzungen angemeldeter Benutzer beenden.

Hauptsystemgehäuse/Hauptsystem

Durch Klicken auf das Objekt **Hauptsystemgehäuse**/**Hauptsystem** können Sie die wichtigen Hardware- und Softwarekomponenten des Systems verwalten.

Die verfügbaren Komponenten sind:

- Batterien
- BIOS
- Lüfter
- Firmware
- Hardware Performance
- Eingriff
- Speicher
- Netzwerk
- Anschlüsse
- Stromverwaltung
- Netzteile
- Prozessoren

- Remote-Zugriff
- Wechselbarer Flash-Datenträger
- Steckplätze
- Temperaturen
- Spannungen

 ANMERKUNG: Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

Eigenschaften des Hauptsystemgehäuses/Hauptsystems

Das System/Servermodul kann ein Hauptsystemgehäuse oder mehrere Gehäuse enthalten. Das Hauptsystemgehäuse/Hauptsystem enthält die wichtigsten Komponenten eines Systems. Das Maßnahmenfenster des Objekts **Hauptsystem Gehäuse/Hauptsystem** umfasst Folgendes:

Eigenschaften

Unterregister: Funktionszustand | Informationen | Systemkomponenten (FRU) | Vorderes Bedienfeld

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- Den Zustand oder Status von Hardwarekomponenten und Sensoren anzeigen. Jede aufgelistete Komponente hat ein Symbol System/Servermodul-Komponentenstatusanzeigen neben der Bezeichnung. gibt an, dass eine Komponente funktionsfähig ist (normal). gibt an, dass sich eine Komponente im Warnzustand (nicht-kritisch) befindet und sofortige Aufmerksamkeit erfordert.  gibt an, dass sich eine Komponente in einem (kritischen) Fehler-Zustand befindet und sofortige Aufmerksamkeit erfordert. gibt an, dass der Funktionszustand der Komponente nicht bekannt ist. Die verfügbaren überwachten Komponenten umfassen:
  - Batterien
  - Lüfter
  - Hardwareprotokoll
  - Eingriff
  - Netzwerk
  - Stromverwaltung
  - Netzteile
  - Prozessoren
  - Temperaturen
  - Spannungen

 ANMERKUNG: Die Funktionen für die **Netzteil-** und die **Stromversorgungsüberwachung** sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

ANMERKUNG: Wenn die QLogic QLE2460 4GB Single-Port Fibre Channel HBA-, QLogic QLE2462 4GB Dual-Port Fibre Channel HBA-, Qlogic QLE2562 Dual Port FC8 Adapter- oder Qlogic QLE2560 Single Port FC8 Adapter-Karten installiert sind, wird der Bildschirm **Systemkomponenten (FRU)** nicht angezeigt.

- Informationen über die Attribute des Hauptsystemgehäuses, wie z.B. den Host-Namen, die iDRAC-Version, Lifecycle Controller-Version, das Gehäuse-Modell, Gehäuseschloss, die Service-Tag-Nummer des Gehäuses, Express-Servicecode und Gehäusesystemkennnummer anzeigen. Das Attribut "Express-Servicecode (ESC)" ist eine 11-stellige "nur-numerische" Konvertierung der Service-Tag-Nummer des Dell-Systems. Während Sie den technischen Support von Dell anrufen, können Sie die Taste <Esc> für Auto-Call-Routing drücken.
- Detaillierte Informationen über die in Ihrem System eingebauten vor Ort austauschbaren Einheiten (FRUs) anzeigen (im Unterregister **Systemkomponenten** (**FRU**)).
- Aktivieren oder deaktivieren Sie die Schaltflächen am vorderen Bedienfeld des verwalteten Systems, und zwar den Netzschalter und die Schaltfläche Nicht-maskierbarer Interrupt (NMI) (falls auf dem System vorhanden). Wählen Sie außerdem die Zugriffsebene für die LCD-Sicherheit des verwalteten Systems aus. Die LCD-Informationen des verwalteten Systems stehen im Drop-Down-Menü zur Auswahl zur Verfügung. Sie können auch die Indikation von Remote-KVM-Sitzung über das Unterregister **Vorderes Bedienfeld** aktivieren.

Batterien

Klicken Sie auf das Objekt **Batterien**, um Informationen über die jeweiligen auf dem System installierten Batterien anzuzeigen. Batterien behalten die Zeit und das Datum bei, wenn das System ausgeschaltet wird. Die Batterie speichert die BIOS-Setup-Konfiguration des Systems, wodurch das System effizient neu gestartet werden kann. Das Maßnahmenfenster des Batterien-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Akkus

Im Register **Eigenschaften** können Sie die aktuellen Messwerte und den Status Ihrer Systembatterien anzeigen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen.
- Konfigurieren Sie die Warnungen, die im Falle einer Batteriewarnung oder eines kritischen/ Fehlerereignisses ausgegeben werden sollen.

BIOS

Klicken Sie auf das Objekt **BIOS**, um die Schlüsselfunktionen des BIOS Ihres Systems zu verwalten. Das System-BIOS enthält auf einem Flash-Speicherchipsatz gespeicherte Programme, die den Datenaustausch zwischen dem Mikroprozessor und Peripheriegeräten, z. B. Tastatur und Videoadapter, und verschiedenen anderen Funktionen, wie z. B. Systemmeldungen, steuern. Das Maßnahmenfenster des Objekts **BIOS** kann, abhängig von den Gruppenberechtigungen des Benutzers, die folgenden Registerkarten aufweisen:

Eigenschaften und **Setup**.

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie BIOS-Informationen anzeigen.

Einrichtung

Unterregister: BIOS

 ANMERKUNG: Das Register "BIOS-Setup" für Ihr System zeigt nur die BIOS-Funktionen an, die auf Ihrem System unterstützt werden.

Im Register **Setup** kann der Zustand jedes BIOS-Setup-Objektes eingestellt werden.

Sie können den Zustand von vielen BIOS-Setup-Funktionen modifizieren, einschließlich, aber nicht beschränkt auf, die serielle Schnittstelle, Festplattenlaufwerkssequenz, benutzerzugängliche USB-Schnittstellen, CPU Virtualization Technology, CPU-Hyperthreading, Netzstromwiederherstellungsmodus, Integrierter SATA-Controller, Systemprofil, Konsolenumleitung und Failsafe-BAUD-Rate der Konsolenumleitung. Sie können auch Folgendes konfigurieren: ein internes USB-Gerät, Einstellungen des Controllers des optischen Laufwerks, den Watchdog-Zeitgeber der automatischen Systemwiederherstellung (ASR), einen integrierten Hypervisor sowie zusätzliche LAN-Netzwerkschnittstellen für Hauptplatineninformationen. Sie können außerdem die Einstellungen von TPM (Trusted Platform Module) und TCM (Trusted Cryptographic Module) anzeigen.

Abhängig von der spezifischen Systemkonfiguration werden eventuell zusätzliche Setup-Elemente angezeigt. Jedoch können einige BIOS-Setup-Optionen auf dem BIOS-Setup-Bildschirm gezeigt werden, die in Server Administrator nicht zugreifbar sind.

Die konfigurierbaren BIOS-Funktionen werden in bestimmte Kategorien gruppiert. Die Kategorien umfassen Debug-Menü, Systeminformationen, Speichereinstellungen, Prozessoreinstellungen, SATA-Einstellungen, Start-Einstellungen, Start-Optionseinstellungen, Netzwerkeinstellungen, integrierte Geräte, Steckplatzdeaktivierung, serielle Kommunikation, Systemprofileinstellungen, Systemsicherheit und verschiedene Einstellungen. Wenn Sie beispielsweise auf der Seite **System-BIOS-Einstellungen** auf den Link **Speichereinstellungen** klicken, werden die Funktionen angezeigt, die zum Systemspeicher gehören. Sie können die Einstellungen anzeigen und bearbeiten, indem Sie zwischen den entsprechenden Kategorien navigieren.

Sie können auf der Seite **Systemsicherheit** ein BIOS-Setup-Kennwort festlegen. Wenn Sie ein Setup-Kennwort festgelegt haben, geben Sie das Kennwort ein, um die BIOS-Einstellungen zu aktivieren und zu ändern. Ansonsten werden die BIOS-Einstellungen im schreibgeschützten Modus angezeigt. Nach der Festlegung des Kennworts müssen Sie das System neu starten.

Wenn offene Werte aus der vorherigen Sitzung vorhanden sind oder die bandinterne Konfiguration durch eine bandexterne Schnittstelle deaktiviert wurde, wird die BIOS-Setup-Konfiguration durch den Server-Administrator nicht genehmigt.

 ANMERKUNG: Die NIC-Konfigurationsinformationen innerhalb des Server Administrator BIOS-Setups sind für integrierte NICs eventuell ungenau. Das Verwenden des BIOS-Setup-Bildschirms, um NICs zu aktivieren oder zu deaktivieren, führt eventuell zu unerwarteten Ergebnissen. Es wird empfohlen, dass Sie alle Konfigurationen für integrierte NICs über den betreffenden System-Setup-Bildschirm ausführen, der während des Systemstarts durch Drücken von <F2> aufgerufen werden kann.

Lüfter

Klicken Sie auf das Objekt **Lüfter**, um Ihre Systemlüfter zu verwalten. Server Administrator überwacht den Status jedes Systemlüfters durch Messung der Lüfterumdrehungen pro Minute. Lüftersonden melden die Lüfterdrehzahlen an den Server Administrator-Instrumentierungsdienst.

Wenn Sie Lüfter in der Gerätestruktur wählen, werden Details im Datenbereich im rechten Teil der Server Administrator-Startseite angezeigt. Das Maßnahmenfenster des Lüfter-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Lüftersonden

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- Zeigen Sie die Strommesswerte Ihrer System-Lüftersonden an und geben Sie Minimal- und Maximalwerte für die Lüftersonden-Warnungschwelle ein.



ANMERKUNG: Einige Lüftersondenfelder unterscheiden sich, je nachdem, welche Firmware Ihr System hat, wie BMC oder ESM. Einige Schwellenwerte können in BMC-Systemen nicht geändert werden.

- Lüftersteuerungsoptionen auswählen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Lüfter einen Warnungs- oder Ausfallwert sendet.
- Stellen Sie die Warnungsschwellenwerte für Lüfter ein.

Firmware

Klicken Sie auf das Objekt **Firmware,** um Ihre Systemfirmware zu verwalten. Firmware besteht aus Programmen oder Daten, die in den ROM geschrieben wurden. Die Firmware kann ein Gerät starten und betreiben. Jeder Controller enthält Firmware, die die Controller-Funktionalität bereitstellt.
Das Maßnahmenfenster des **Firmware**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie die Firmware-Informationen für das System anzeigen.

Hardware Performance

Klicken Sie auf das Objekt **Hardwareleistung**, um den Status und die Ursache für den Abfall der Systemleistung anzuzeigen. Das Maßnahmenfenster des **Hardwareleistung**-Objekts kann, abhängig von den Gruppen Berechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie die Details zur Verschlechterung der Systemleistung sehen.

In der folgenden Tabelle werden die möglichen Werte für den Status und die Ursache einer Sonde aufgelistet:

Tabelle 9. Mögliche Werte für den Status und die Ursache einer Sonde

Statuswerte	Ursachenwerte
Herabgesetzt	Benutzerkonfiguration Unzureichende Stromkapazität Grund ist nicht bekannt
Normal	k.A.

Eingriff

Klicken Sie auf das Objekt **Eingriff**, um den Gehäuseeingriffsstatus Ihres Systems zu verwalten. Server Administrator überwacht den Gehäuseeingriffsstatus als Sicherheitsmaßnahme zur Vermeidung unbefugten Zugriffs auf die kritischen Komponenten des Systems. Gehäuseeingriff zeigt an, dass jemand die Abdeckung des Systemgehäuses öffnet oder bereits geöffnet hat. Das Maßnahmenfenster des **Eingriff**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, folgende Register aufweisen: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Eingriff

Im Register **Eigenschaften** können Sie den Gehäuseeingriffsstatus anzeigen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn der Eingriffssensor einen Warnungs- oder Ausfallwert sendet.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für den Eingriffssensor festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

Speicher

Klicken Sie auf das Objekt **Speicher**, um die Speichergeräte des Systems zu verwalten. Server Administrator überwacht den Speichergerätestatus für jedes im überwachten System vorhandene Speichermodul. Speichergerät-Vorfehlersensoren überwachen die Speichermodule durch Zählen der ECC-Speicherkorrekturen. Server Administrator überwacht auch Speicherredundanzinformationen, falls

das betreffende System diese Funktion unterstützt. Das Maßnahmenfenster des Objekts **Speicher** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Speicher

Auf der Registerkarte **Eigenschaften** können Sie den Speicherredundanzstatus, die Speicher-Array-Attribute, die Gesamtkapazität der Speicher-Arrays, die Details der Speicher-Arrays, die Speichergerätedetails sowie den Speichergerätestatus abrufen. Die Details des Speichergeräts geben die Details eines Speichergeräts wie Status, Gerätename, Größe, Typ, Taktrate, Rang und Fehler auf einem Konnekt an. Ein Rang ist eine Reihe von dynamischen Speicher mit wahlfreiem Zugriff, der aus 64 Datenbits pro DIMM-Speichermodule besteht. Die möglichen Werte von Rang sind `single, dual, quad, octal,` (Einzel, Zweifach, Vierfach, Achtfach) und `hexa` (Hexa). Der Rang zeigt den Rang von DIMM an und hilft mit der leichten Dienstleistung von DIMMs auf dem Server.



ANMERKUNG: Wenn ein System mit aktiviertem Spare Bank-Speicher in einen "Redundanz verloren"-Zustand übergeht, ist es eventuell nicht offensichtlich, welches Speichermodul die Ursache ist. Wenn Sie nicht bestimmen können, welches DIMM ersetzt werden muss, prüfen Sie den Protokolleintrag *Wechsel zu Ersatzspeicherbank festgestellt* im ESM-Systemprotokoll, um herauszufinden, welches Speichermodul versagte.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Speichermodul einen Warnungs- oder Ausfallwert sendet.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für Speichermodule festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

Netzwerk

Klicken Sie auf das **Netzwerk**-Objekt, um die NICs des Systems zu verwalten. Der Server Administrator überwacht den Status jedes NIC im System, um eine kontinuierliche Remoteverbindung zu gewährleisten. Der Server Administrator berichtet FCoE- und iSoE-Fähigkeiten des NICs. Des Weiteren wird über NIC-Teamingdetails Bericht erstattet, wenn diese bereits auf dem System konfiguriert wurden. Zwei oder mehrere physische NICs können zu einem einzigen logischen NIC kombiniert werden, dem ein Administrator eine IP-Adresse zuweisen kann. Teaming kann unter Verwendung von NIC-Herstellerhilfsprogrammen konfiguriert werden. Beispiel: Broadcom – BACS. Wenn einer der physischen NICs ausfällt, kann weiterhin auf die IP-Adresse zugegriffen werden, da sie an den logischen NIC und nicht an einen einzigen physischen NIC gebunden ist. Wenn die Teamschnittstelle konfiguriert ist, werden die Teameigenschaften im Detail angezeigt. Die Beziehung zwischen physischen NICs und Teamschnittstellen bzw. umgekehrt wird ebenfalls gemeldet, wenn diese physischen NICs Mitglieder der Teamschnittstelle sind.

Auf einem Windows2008 Hypervisor-Betriebssystem meldet der Server-Administrator die IP-Adressen der physikalischen NIC-Schnittstellen, die zur Zuordnung eines IP zu einem virtuellen Computer verwendet werden, nicht.

 ANMERKUNG: Dass die Reihenfolge, in der Geräte erkannt werden, der physikalischen Anordnung der Ports am Gerät entspricht, ist nicht gewährleistet. Klicken Sie auf den Hyperlink unter der Schnittstellennamen, um die NIC-Informationen abzurufen.

In ESXi-Betriebssystemen wird das Netzwerkgerät als Gruppe betrachtet. Beispiele: Die virtuelle Ethernet-Schnittstelle, die durch die Dienstkonsole (vswif) verwendet wird und die virtuelle Netzwerkschnittstelle, die durch das vmknic-Gerät auf ESXi verwendet wird.

Das Maßnahmenfenster des **Netzwerk**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

Über das Register **Eigenschaften** können Sie Informationen zu den auf dem System installierten physischen NIC-Schnittstellen als auch Teamschnittstellen anzeigen.

 ANMERKUNG: Im Abschnitt der IPv6-Adressen zeigt Server Administrator neben der Link-local-Adresse nur zwei Adressen an.

 ANMERKUNG: Auf Systemen mit Linux Betriebssystemen mit Kernel-Versionen, die älter als 3.10 sind, wird Team Interface-Geschwindigkeit nicht angezeigt.

Anschlüsse

Klicken Sie auf das **Schnittstellen**-Objekt, um die externen Anschlüsse des Systems zu verwalten. Server Administrator überwacht den Status jeder im System vorhandenen externen Schnittstelle.

 ANMERKUNG: CMC USB-Schnittstellen mit angeschlossenen Blade-Servern werden von OMSA nicht aufgelistet.

Das Maßnahmenfenster des **Schnittstellen**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

Unterregister: Informationen

Eigenschaften

Im Register **Eigenschaften** können Sie die Informationen über die im System vorhandenen externen Schnittstellen anzeigen.

Stromverwaltung

 ANMERKUNG: Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

Überwachung

Unterregister: Verbrauch | Statistik

Im Register **Verbrauch** können Sie die Leistungsaufnahmeinformationen des System in Watt und BTU/h anzeigen und verwalten.

BTU/h = Watt X 3,413 (Wert zur nächsten ganzen Zahl abgerundet)

Server Administrator überwacht den Stromverbrauchstatus, die Stromstärke und Details zur Stromstatistik.

Sie können auch den Sofort-Toleranzbereich des Systems sowie den Spitzen-Toleranzbereich des Systems anzeigen. Die Werte werden sowohl in Watt als auch in BTU/h (British Thermal Unit) angezeigt. Stromschwellenwerte können sowohl in Watt als auch in BTU/h festgelegt werden.

Über das Register „Statistik" können Sie die Stromverfolgungsstatistik des Systems anzeigen und zurücksetzen, wie z. B. für Energieverbrauch, Spitzenleistung des Systems und Spitzenstromstärke des Systems.

Verwaltung

Unterregister: Budget | Profile

Über das Register **Budget** können Sie die Strominventarattribute wie Spannungslosigkeit des Systems und den maximalen potenziellen Systemstrom in Watt und BTU/h anzeigen. Sie können die Strombudget-Option auch dazu verwenden, die Stromobergrenze zu aktivieren und die Stromobergrenze für das System festzulegen.

Über das Register **Profile** können Sie ein Stromprofil auswählen, um die Systemleistung zu maximieren und Energie einzusparen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Verwenden Sie das Register **Warnungsmaßnahmen**, um Systemwarnungsmaßnahmen für verschiedene Systemereignisse wie Systemstromsondenwarnungen und Spitzenleistung des Systems festzulegen.

Verwenden Sie das Register **SNMP-Traps** zum Konfigurieren von SNMP-Traps für das System.

Bestimmte Energieverwaltungs-Funktionen stehen eventuell nur auf Systemen zur Verfügung, die mit dem Energieverwaltungs-Bus (PMBus) aktiviert wurden.

Netzteile

Klicken Sie auf das **Netzteile**-Objekt, um die Netzteile des Systems zu verwalten. Server Administrator überwacht den Status der Netzteile, einschließlich der Redundanz, um sicherzustellen, dass jedes im System vorhandene Netzteil korrekt funktioniert.

Das Maßnahmenfenster des Objekts Netzteile kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

ANMERKUNG: Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

Eigenschaften

Unterregister: Elemente

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- Informationen über die Attribute der Netzteilredundanz anzeigen.
- Überprüfen Sie den Status der einzelnen Netzteilkomponenten, einschließlich der Firmware-Version des Netzteils und der maximalen Ausgangswattleistung.
- Überprüfen Sie den Status der einzelnen Netzteilkomponenten, einschließlich der Firmware-Version des Netzteils, der Nenn-Eingangswattleistung und der maximalen Ausgangswattleistung.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register Warnungsverwaltung können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemstrom einen Warnungs- oder Ausfallwert sendet.
- Plattformereignis-Warnungsziele für IPv6-Adressen konfigurieren.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für Systemleistung (Watt) festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.



ANMERKUNG: Der Trap für den Spitzenstrom des Systems erzeugt nur Ereignisse für die Schweregradstufe "Zur Information".

Prozessoren

Klicken Sie auf das Objekt **Prozessoren**, um die Mikroprozessoren des Systems zu verwalten. Ein Prozessor ist der primäre Rechenchip im Inneren eines Systems, der die Auswertung und Ausführung von arithmetischen und logischen Funktionen steuert. Das Maßnahmenfenster des Prozessor-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Unterregister: Informationen

Eigenschaften

Im Register **Eigenschaften** können Sie Informationen über den/die Mikroprozessor(en) des Systems anzeigen und auf detaillierte Informationen des Cache zugreifen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen

Im Register **Warnungsverwaltung** können Sie die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Prozessor einen Warnungs- oder Ausfallwert sendet.

Remote-Zugriff

Klicken Sie auf das Objekt **Remote-Zugriff**, um die BMC-Funktionen Baseboard Management Controller) oder iDRAC-Funktionen (Integrated Dell Remote Access Controller) und Remote Access Controller-Funktionen zu verwalten.

Durch die Auswahl des Registers "Remote-Zugriff" können Sie die BMC/iDRAC-Funktionen, wie z. B. allgemeine Informationen zu BMC/iDRAC, verwalten. Sie können auch die Konfiguration des BMC/iDRAC in einem LAN-Netzwerk, die serielle Schnittstelle für den BMC/iDRAC, Terminalmoduseinstellungen für die serielle Schnittstelle, BMC/iDRAC seriell über LAN und BMC/iDRAC-Benutzer verwalten.



ANMERKUNG: Wenn eine andere Anwendung als Server Administrator zur Konfiguration des BMC/iDRAC verwendet wird, während Server Administrator läuft, dann kann es vorkommen, dass die BMC/iDRAC-Konfigurationsdaten, die von Server Administrator angezeigt werden, nicht mit dem BMC/iDRAC übereinstimmen. Es wird deshalb empfohlen, Server Administrator zur Konfiguration des BMC/iDRAC zu verwenden, während Server Administrator läuft.

Mit DRAC können Sie auf die Remote System Management-Fähigkeiten des Systems zugreifen. Der Server Administrator DRAC bietet Remote-Zugriff auf nicht arbeitsfähige Systeme, Warnungsmeldungen, wenn ein System außer Betrieb ist, und die Möglichkeit, ein System neu zu starten.

Das Maßnahmenfenster des **Remote-Zugriff-**Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, folgende Register aufweisen: **Eigenschaften, Konfiguration** und **Benutzer.**

Unterregister: Informationen

Eigenschaften

Im Register **Eigenschaften** können Sie allgemeine Informationen über das Remote-Zugriffsgerät anzeigen. Sie können auch die Attribute der IPv4- und IPv6-Adressen anzeigen.

Klicken Sie auf **Auf Standardeinstellungen zurücksetzen**, um alle Attribute wieder auf ihre Standardeinstellungen zurückzusetzen.

Unterregister: LAN | Serielle Schnittstelle | Seriell über LAN |Zusätzliche Konfiguration

Konfiguration

Wenn BMC/iDRAC konfiguriert ist, können Sie im Register Konfiguration den BMC/iDRAC für ein LAN-Netzwerk, die serielle Schnittstelle für den BMC/iDRAC oder den BMC/iDRAC seriell über LAN konfigurieren.



ANMERKUNG: Das Register Zusätzliche Konfiguration steht nur auf Systemen mit iDRAC zur Verfügung.

Wenn DRAC konfiguriert ist, können Sie auf der Registerkarte **Konfiguration** Netzwerkeinstellungen konfigurieren.

Im Register **Zusätzliche Konfiguration** können Sie IPv4/IPv6-Eigenschaften aktivieren oder deaktivieren.

ANMERKUNG: Das Aktivieren/Deaktivieren von IPv4/IPv6 ist nur in einer Dual-Stack-Umgebung möglich (wo sowohl die IPv4- als auch die IPv6-Stacks geladen sind).

Benutzer

Unterregister: Benutzer

Im Register **Benutzer** kann die Benutzerkonfiguration für Remote-Zugriff geändert werden. Informationen über Remote Access Controller-Benutzer können hinzugefügt, konfiguriert und angezeigt werden.

Wechselbarer Flash-Datenträger

Klicken Sie auf das Objekt **Wechselbarer Flash-Datenträger**, um den Funktionszustand und Redundanzstatus interner SD-Module und vFlash-Datenträger anzuzeigen. Das Maßnahmenfenster des wechselbaren Flash-Datenträgers verfügt über das Register **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie Informationen zu den wechselbaren Flash-Datenträgern und internen SD-Modulen anzeigen. Dies schließt Details zum Konnektornamen, dessen Zustand sowie seiner Speichergröße ein.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, falls die wechselbare Flash-Datenträgersonde einen Warnungs- oder Ausfallwert zurückgibt.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für wechselbare Flash-Datenträgersonden festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

Interne SD-Module und vFlash nutzen die Warnungsverwaltung gemeinsam. Durch die Konfiguration von Warnungsmaßnahmen/SNMP/PEF für die SD-Module oder für vFlash werden diese automatisch für die jeweils andere Option konfiguriert.

Steckplätze

Klicken Sie auf das Objekt **Steckplätze**, um die Anschlüsse oder Sockel auf der Hauptplatine zu verwalten, die gedruckte Leiterplatinen, wie z. B. Erweiterungskarten, aufnehmen. Das Maßnahmenfenster Steckplätze-Objekts enthält das Register **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie Informationen über jeden Steckplatz und installierten Adapter anzeigen.

Temperaturen

Klicken Sie auf das Objekt **Temperaturen**, um die Systemtemperatur zu verwalten und Hitzeschäden an den internen Komponenten zu verhindern. Server Administrator überwacht die Temperatur an verschiedenen Stellen im Systemgehäuse, um sicherzustellen, dass die Temperaturen im Gehäuse nicht zu hoch sind.

Das Maßnahmenfenster des Objekts **Temperaturen** weist die folgenden Register auf, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Unterregister: Temperatursonden

Auf der Registerkarte **Eigenschaften** können Sie die Strommesswerte und den Status der Temperatursonden des Systems abrufen und Minimal- und Maximalwerte für den Schwellenwert der Temperatursonden-Warnung angeben.



ANMERKUNG: Einige Temperatursondenfelder weichen ab, je nachdem, welche Firmware Ihr System hat wie BMC oder ESM. Einige Schwellenwerte können in BMC-Systemen nicht geändert werden. Beim Zuweisen von Sondenschwellenwerten rundet Server Administrator die von Ihnen eingegebenen Minimal- oder Maximalwerte manchmal auf die am nächsten zuweisbaren Werten.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn eine Temperatursonde einen Warnungs- oder Ausfallwert sendet.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für Temperatursonden festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.



ANMERKUNG: Sie können minimale und maximale Schwellenwerte der Temperatursonde für ein externes Gehäuse nur in Ganzzahlen angeben. Wenn Sie versuchen, den minimalen oder maximalen Schwellenwert der Temperatursonde auf einen Dezimalwert zu setzen, wird nur die Ganzzahl vor dem Komma als Schwellenwerteinstellung gespeichert.

Spannungen

Klicken Sie auf das Objekt **Spannungen**, um die Spannungsniveaus im System zu regeln. Server Administrator überwacht die Spannungen in kritischen Komponenten an verschiedenen Gehäusestellen im überwachten System. Das Maßnahmenfenster des **Spannungen**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Spannungssonden

Auf der Registerkarte **Eigenschaften** können Sie die Strommesswerte und den Status der Temperatursonden Ihres Systems ablesen und die Minimal- und Maximalwerte, d. h. die Schwellenwerte für die Temperatursonden-Warnung, konfigurieren.



ANMERKUNG: Einige Spannungssondenfelder weichen ab, je nachdem, welche Firmware Ihr System hat, wie BMC oder ESM. Einige Schwellenwerte können in BMC-Systemen nicht geändert werden.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- Sehen Sie die aktuellen Warnungsmaßnahmen-Einstellungen, und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemspannungssensor einen Warnungs- oder Ausfallwert sendet.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für Spannungssensoren festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

Software

Klicken Sie auf das Objekt **Software**, um detaillierte Versionsinformationen über die wichtigsten Softwarekomponenten des verwalteten Systems anzuzeigen, z. B. das Betriebssystem und die Systemverwaltungssoftware. Das Maßnahmenfenster des Software-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

Unterregister: Zusammenfassung

Eigenschaften

Im Register **Eigenschaften** können Sie eine Zusammenfassung über Betriebssystem und Systemverwaltungssoftware des überwachten Systems anzeigen.

Betriebssystem

Klicken Sie auf das Objekt **Betriebssystem**, um grundlegende Informationen über das jeweilige Betriebssystem anzuzeigen. Das Maßnahmenfenster des Betriebssystem-Objekts kann das folgende Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie grundlegende Informationen über das jeweilige Betriebssystem anzeigen.

Bei Lagerung

Server Administrator enthält den Storage Management-Dienst:

Der Storage Management-Dienst enthält Funktionen für die Konfiguration der Speichergeräte. In den meisten Fällen wird der Storage Management-Dienst unter Verwendung des **typischen Setups** installiert. Der Storage Management-Dienst ist auf den Betriebssystemen Microsoft Windows, Red Hat Enterprise Linux und SUSE Linux Enterprise Server verfügbar.

Wenn Storage Management-Dienst installiert ist, klicken Sie auf das Objekt **Speicher**, um den Status und die Einstellungen für verschiedene angeschlossene Array-Speichergeräte, Datenträger, Systemfestplatten usw. anzuzeigen.

Beim Storage Management-Dienst hat das Maßnahmenfenster des Speichermedien-Objekts, je nach Gruppenberechtigungen des Benutzers, folgende Register: **Eigenschaften**.

Eigenschaften

Unterregister: Funktionszustand

Im Register **Eigenschaften** können Sie den Funktionszustand oder Status angeschlossener Speicherkomponenten und Sensoren wie Array-Subsysteme, Betriebssystem-Festplatten und Datenträger anzeigen.

Voreinstellungen verwalten: Konfigurationsoptionen der Homepage

Im linken Fenster der **Einstellungen**-Startseite (in der die Systemstruktur auf der Startseite von Server Administrator angezeigt wird) werden alle verfügbaren Konfigurationsoptionen im Systemstrukturfenster angezeigt. Die angezeigten Optionen basieren auf der Systemverwaltungssoftware, die auf dem verwalteten System installiert ist.

Die verfügbaren Konfigurationsoptionen der **Einstellungen**-Startseite sind:

- Allgemeine Einstellungen
- Server Administrator

Allgemeine Einstellungen

Klicken Sie auf das Objekt **Allgemeine Einstellungen**, um Benutzer- und DSM SA Verbindungsdienst-Einstellungen (Web Server) für ausgewählte Server Administrator-Funktionen einzurichten. Das Maßnahmenfenster des Allgemeine Einstellungen-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Benutzer** und **Web Server**.

Unterregister: Eigenschaften

Benutzer

Im Register **Benutzer** können Sie Benutzereinstellungen festlegen z. B. die Startseite-Darstellung und die Standard-E-Mail-Adresse für die Schaltfläche **E-Mail**.

- **Webserver**
- **Unterregister: Eigenschaften | X.509-Zertifikat**

Im Register Web Server können Sie Folgendes durchführen:

- DSM SA-Verbindungsdiensteinstellungen festlegen. Anweisungen zum Konfigurieren von Servereinstellungen finden Sie unter Dell Systems Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup
- Konfigurieren Sie die SMTP-Serveradresse und die Bind-IP-Adresse entweder im IPv4- oder IPv6-Adressierungsmodus.
- Führen Sie die X.509-Zertifikatsverwaltung durch, indem Sie ein neues X.509-Zertifikat erzeugen, ein vorhandenes X.509-Zertifikat wiederverwenden oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) importieren. Weitere Informationen zur Zertifikatsverwaltung finden Sie unter X.509-Zertifikatsverwaltung.

Server Administrator

Klicken Sie auf das **Server Administrator**-Objekt, um den Zugriff von Benutzern mit Benutzer- oder Hauptbenutzer-Berechtigungen zu aktivieren oder deaktivieren. Das Maßnahmenfenster des **Server Administrator**-Objekts kann das folgende Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften**.

Unterregister: Zugriffskonfiguration

Einstellungen

Im Register **Einstellungen** können Sie den Zugriff auf Benutzer mit Benutzer- oder Hauptbenutzer-Berechtigungen aktivieren oder deaktivieren.

5

Arbeiten mit dem Remote Access Controller

Der Dell BMC/iDRAC (Baseboard Management Controller/Integrated Dell Remote Access Controller) überwacht das System auf kritische Ereignisse, indem er mit verschiedenen Sensoren auf der Systemplatine kommuniziert und Warnungen und Protokollereignisse sendet, wenn bestimmte Parameter die voreingestellten Schwellenwerte überschreiten. Der BMC/iDRAC unterstützt die Industriestandards von Intelligent Platform Management Interfaces (IPMI), sodass Sie Systeme im Remote-Zugriff konfigurieren, überwachen und wiederherstellen können.

Der DRAC ist eine Hardware- und Softwarelösung zur Systemverwaltung und bietet Remote-Verwaltung, Wiederherstellung eines abgestürzten Systems sowie Stromsteuerungsfunktionen für Dell-Systeme.

Durch die Kommunikation mit dem BMC/iDRAC (Baseboard Management Controller/Integrated Dell Remote Access Controller) des Systems kann der DRAC für das Senden von E-Mail-Warnungen mit Warn- oder Fehlermeldungen zu Spannung, Temperatur und Lüftergeschwindigkeit konfiguriert werden. Der DRAC protokolliert außerdem Ereignisdaten und den letzten Bildschirm vor dem Absturz (nur auf Systemen verfügbar, die das Betriebssystem Microsoft Windows ausführen), um Ihnen bei der Diagnose der wahrscheinlichen Ursache eines Systemabsturzes behilflich zu sein.

Der Remote Access Controller gestattet externen Zugriff auf ein nicht funktionierendes System, wodurch es schnellstmöglich wieder in einen funktionierenden Zustand versetzt werden kann. Der Remote Access Controller bietet darüber hinaus Warnungsbenachrichtigung, wenn ein System ausgefallen ist, und ermöglicht den Neustart eines Systems im Remote-Zugriff. Darüber hinaus protokolliert der Remote Access Controller die wahrscheinliche Ursache von Systemabstürzen und speichert den *letzten Bildschirm vor dem Absturz*.

Sie können sich beim Remote Access Controller anmelden, entweder über die Server Administrator-Startseite oder durch direktes Zugreifen auf die IP-Adresse des Controllers mit einem unterstützen Browser.

Bei der Verwendung des Remote Access Controllers können Sie auf **Hilfe** klicken, um detaillierte Informationen über das Fenster zu erhalten, in dem Sie sich gerade befinden. Remote Access Controller-Hilfe ist in allen Fenstern verfügbar, die dem Benutzer zugänglich sind, basierend auf den entsprechenden Zugriffsrechten und den spezifischen Hardware- und Softwaregruppen, die der Server Administrator auf dem verwalteten System feststellt.

 ANMERKUNG: Weitere Informationen über BMC finden Sie im *Dell OpenManage Baseboard Management Controller User's Guide* (Benutzerhandbuch für Dell OpenManage Baseboard-Verwaltungs-Controller) unter dell.com/systemsecuritymanuals.

 ANMERKUNG: Weitere Informationen zur Verwendung von DRAC 5 finden Sie im *Dell Remote Access Controller 5 User’s Guide* (Dell Remote Access Controller 5-Benutzerhandbuch) unter dell.com/systemsecuritymanuals.

 ANMERKUNG: Ausführliche Informationen über das Konfigurieren und Verwenden des iDRAC finden Sie im *Integrated Dell Remote Access Controller User's Guide* (Benutzerhandbuch zum Integrated Dell Remote Access Controller) unter **dell.com/systemsecuritymanuals**.

Die folgende Tabelle listet die Feldnamen und das zutreffende System der grafischen Benutzerschnittstelle (GUI) auf, wenn Server Administrator auf dem System installiert ist.

Tabelle 10. GUI Feldnamen und das zutreffende System

Feldname der Benutzeroberfläche	Entsprechendes System
Modulares Gehäuse	Modulares System
Servermodule	Modulares System
Hauptsystem	Modulares System
System	Nicht modulares System
Hauptsystemgehäuse	Nicht modulares System

Weitere Informationen zur Systemunterstützung für Geräte mit Remote-Zugriff finden Sie unter *Dell Systems Software Support Matrix*, das unter **dell.com/openmanagemanuals** verfügbar ist.

Server Administrator ermöglicht den bandinternen Remote-Zugriff auf Ereignisprotokoll-, Stromsteuerungs- und Sensorstatusdaten und die Konfiguration des BMC/iDRAC. Sie können den BMC/iDRAC und den DRAC über die grafische Benutzeroberfläche von Server Administrator verwalten, indem Sie auf das Objekt **Remote-Zugriff** klicken, das eine Unterkomponente der Gruppe **Hauptsystemgehäuse/Hauptsystem** ist.

Sie können folgende Aufgaben ausführen:

- Anzeigen grundlegender Informationen
- Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer LAN-Verbindung
- Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer Seriell-über-LAN-Verbindung
- Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer seriellen Schnittstellenverbindung
- Zusätzliche Konfiguration für iDRAC
- Konfigurieren der Benutzer von Remote-Zugriffsgeräten
- Plattformereignisfilter-Warnungen einstellen

Sie können BMC/iDRAC- oder DRAC-Informationen basierend auf der Hardware anzeigen, die die Remote-Zugriffsfunktionen für das System bietet.

Berichterstattung und Konfiguration von BMC/iDRAC und DRAC können auch mit Hilfe des CLI-Befehls `omreport/omconfig chassis remoteaccess` verwaltet werden.

Außerdem können Sie den Server Administrator Instrumentation Service für die Verwaltung der Parameter und Warnungsziele des Plattformereignisfilters (PEF) verwenden.

Anzeigen grundlegender Informationen

Sie können grundlegende Informationen zu zum BMC/iDRAC, zur IPv4-Adresse und zum DRAC anzeigen. Sie haben auch die Möglichkeit, die Einstellungen des Remote Access Controllers auf die Standardwerte zurückzusetzen. Führen Sie dazu folgende Schritte durch:



ANMERKUNG: Um die BMC-Einstellungen einzustellen, müssen Sie mit Admin-Zugriffsrechten angemeldet sein.

Klicken Sie auf **Modulares Gehäuse** → **System/Servermodul** → **Hauptsystemgehäuse/Hauptsystem** → **Remote-Zugriff**.

Die Seite **Remote-Zugriff** zeigt folgende grundlegende Informationen für den System-BMC an:

Remote-Zugriffsgerät

- Gerätetyp
- IPMI-Version
- System-GUID
- Anzahl von möglichen aktiven Sitzungen
- Anzahl von aktuellen aktiven Sitzungen
- LAN aktiviert
- SOL aktiviert
- MAC-Adresse

IPv4-Adresse

- IP-Adressen-Quelle
- IP-Adresse
- IP-Subnetz
- IP-Gateway

IPv6-Adresse

- IP-Adressen-Quelle
- IPv6-Adresse 1
- Standard-Gateway
- IPv6-Adresse 2
- Link-Local-Adresse
- DNS-Adressquelle
- Bevorzugter DNS-Server
- Alternativer DNS-Server



ANMERKUNG: Details zu den IPv4- und IPv6-Adressen können nur angezeigt werden, wenn Sie die IPv4- und IPv6-Adresseneigenschaften im Register **Remote-Zugriff** unter **Zusätzliche Konfiguration** aktivieren.

Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer LAN-Verbindung

So konfigurieren Sie das Remote-Zugriffsgerät für die Kommunikation über eine LAN-Verbindung:

1. Klicken Sie auf das Objekt **Modulares Gehäuse** → **System/Servermodul** → **Hauptsystemgehäuse/ Hauptsystem** → **Remote-Zugriff** .
2. Klicken Sie auf das Register **Configuration** (Konfiguration).
3. Klicken Sie auf **LAN**.
   Das Fenster **LAN-Konfiguration** wird angezeigt.

   ANMERKUNG: BMC/iDRAC-Verwaltungsverkehr funktioniert nicht richtig, wenn das LAN auf der Hauptplatine (LOM) mit Netzwerkadapter-Add-In-Karten kombiniert wird.
4. Konfigurieren Sie die folgenden NIC-Konfigurationsdetails:
   - NIC aktivieren (Wählen Sie diese Option für das NIC-Teaming aus.)

   ANMERKUNG: Die DRAC enthält einen integrierten 10BASE-T/100BASE-T Ethernet-NIC und unterstützt TCP/IP. Der NIC hat die Standardadresse 192.168.20.1 und den Standard-Gateway 192.168.20.1.

   ANMERKUNG: Wenn der DRAC auf die gleiche IP-Adresse wie ein anderer NIC auf dem gleichen Netzwerk eingestellt ist, tritt ein IP-Adressenkonflikt auf. Der DRAC antwortet nicht mehr auf Netzwerkbefehle, bis die IP-Adresse auf dem DRAC geändert wird. Der DRAC muss selbst dann zurückgesetzt werden, wenn der IP-Adressenkonflikt durch Änderung der IP-Adresse des anderen NIC aufgelöst wird.

   ANMERKUNG: Eine Änderung der IP-Adresse des DRAC bewirkt, dass der DRAC zurückgesetzt wird. Wenn SNMP den DRAC abfragt, bevor er initialisiert wird, wird eine Temperaturwarnmeldung protokolliert, da die korrekte Temperatur erst nach der Initialisierung des DRAC übertragen wird.

     - NIC-Auswahl

   ANMERKUNG: Die NIC-Auswahl kann auf modularen Systemen nicht konfiguriert werden.

   - Primär- und Failover-Netzwerkoptionen

   Die Primärnetzwerkoptionen für die Remote Management (iDRAC7)-NIC sind: LOM1, LOM2, LOM3, LOM4 und Dezidiert . Die Failover-Netzwerkoptionen lautet wie folgt: LOM1, LOM2, LOM3, LOM4, All LOMs und Keine.

   ANMERKUNG: Die Anzahl der LOMs richtet sich nach der System- und Hardware-Konfiguration.

   - IPMI-Über-LAN aktivieren
   - IP-Adressen-Quelle
   - IP-Adresse
   - Subnetzmaske
   - Gateway-Adresse
   - Beschränkung der Kanalberechtigungsebene
5. Konfigurieren Sie die folgenden optionalen VLAN-Konfigurationsdetails:

ANMERKUNG: VLAN-Konfiguration ist nicht anwendbar für Systeme mit iDRAC.

- VLAN-ID aktivieren
- VLAN-ID
- Priorität

6. Konfigurieren Sie die folgenden IPv4-Eigenschaften:
   - IP-Adressen-Quelle
   - IP-Adresse
   - Subnetzmaske
   - Gateway-Adresse
7. Konfigurieren Sie die folgenden IPv6-Eigenschaften:
   - IP-Adressen-Quelle
   - IP-Adresse
   - Präfixlänge
   - Standard-Gateway
   - DNS-Adressquelle
   - Bevorzugter DNS-Server
   - Alternativer DNS-Server

   ANMERKUNG: Details zu den IPv4- und IPv6-Adressen können nur konfiguriert werden, wenn Sie die IPv4- und IPv6-Eigenschaften unter **Zusätzliche Konfiguration** aktivieren.
8. Klicken Sie auf **Änderungen anwenden**.

Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer seriellen Schnittstellenverbindung

So konfigurieren Sie den BMC für die Kommunikation über eine serielle Schnittstellenverbindung:

1. Klicken Sie auf **Modulares Gehäuse** → **System/Servermodul** → **Hauptsystemgehäuse/Hauptsystem** → **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **Serielle Schnittstelle**.

   Das Fenster **Konfiguration der seriellen Schnittstelle** wird angezeigt.
4. Konfigurieren Sie folgende Details:
   - Verbindungsmoduseinstellung
   - Baudrate
   - Datenflusssteuerung
   - Beschränkung der Kanalberechtigungsebene
5. Klicken Sie auf **Änderungen anwenden**.
6. Klicken Sie auf **Terminalmoduseinstellungen**.

   Im Fenster Terminalmoduseinstellungen können Sie die Terminalmoduseinstellungen für die serielle Schnittstelle konfigurieren.

   Der Terminalmodus wird für IPMI-Meldungen (Intelligent Plattform Schnittstellenmanagement) über die serielle Schnittstelle unter Verwendung von druckbaren ASCII-Zeichen benutzt. Der Terminalmodus unterstützt auch eine begrenzte Zahl an Textbefehlen für die Unterstützung

herkömmlicher textbasierter Umgebungen. Diese Umgebung ist so gestaltet, dass ein einfaches Terminal oder ein Terminalemulator verwendet werden kann.

7. Legen Sie folgende benutzerspezifische Daten fest, um die Kompatibilität mit ihren bestehenden Terminals zu erhöhen:
   - Zeilenbearbeitung
   - Löschsteuerung
   - Echo-Steuerung
   - Handshaking-Steuerung
   - Neue Zeilenreihenfolge
   - Neue Zeilenreihenfolge eingeben
8. Klicken Sie auf **Änderungen anwenden**.
9. Klicken Sie auf **Zurück zum Fenster Konfiguration der seriellen Schnittstelle**, um zum Fenster **Konfiguration der seriellen Schnittstelle** zu wechseln.

Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer Seriell-über-LAN-Verbindung

So konfigurieren Sie den BMC/iDRAC für Datenübertragung einer Seriell-über-LAN-Verbindung (SOL):

1. Klicken Sie auf das Objekt **Modulares Gehäuse** → **System/Servermodul** → **Hauptsystemgehäuse/ Hauptsystem** → **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **Seriell über LAN**.

   Das Fenster **Seriell-über-LAN-Konfiguration** wird angezeigt.
4. Konfigurieren Sie folgende Details:
   - Seriell über LAN aktivieren
   - Baudrate
   - Erforderliche Mindestberechtigung
5. Klicken Sie auf **Änderungen anwenden**.
6. Klicken Sie auf **Erweiterte Einstellungen**, um den BMC weiter zu konfigurieren.
7. Im Fenster **Seriell-über-LAN-Konfiguration - Erweiterte Einstellungen** können Sie die folgenden Informationen konfigurieren:
   - Intervall der Zeichenakkumulation
   - Schwellenwert der gesendeten Zeichen
8. Klicken Sie auf **Änderungen anwenden**.
9. Klicken Sie auf **Zurück zu Seriell-über-LAN-Konfiguration**, um zum Fenster **Seriell-über-LAN-Konfiguration** zurückzukehren.

Zusätzliche Konfiguration für iDRAC

So konfigurieren Sie die IPv4- und IPv6-Eigenschaften unter Verwendung der Registerkarte **Zusätzliche Konfiguration**:

1. Klicken Sie auf das Objekt **Modulares Gehäuse System/Servermodul Hauptsystemgehäuse/ Hauptsystem Remote-Zugriff**
2. Klicken Sie auf das Register **Configuration** (Konfiguration).
3. Klicken Sie auf **Zusätzliche Konfiguration**.

4. Konfigurieren Sie die IPv4- und IPv6-Eigenschaften als **Aktiviert** oder **Deaktiviert**.
5. Klicken Sie auf **Änderungen anwenden**.



ANMERKUNG: Weitere Informationen zur Lizenzverwaltung finden Sie im *Dell License Manager User's Guide* (Dell License Manager-Benutzerhandbuch) unter dell.com/openmanagemanuals.

Konfigurieren der Benutzer von Remote-Zugriffsgeräten

So konfigurieren Sie Benutzer von Remote-Zugriffsgeräten über die Seite Remote-Zugriff:

1. Klicken Sie auf das Objekt **Modulares Gehäuse** → **System/Servermodul** → **Hauptsystemgehäuse/ Hauptsystem** → **Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **Benutzer**.

   Im Fenster **Remote-Zugriffsbenutzer** werden Informationen über Benutzer angezeigt, die ein BMC/ iDRAC-Benutzer konfigurieren kann.
3. Klicken Sie auf **Benutzer-ID**, um einen neuen oder bestehenden BMC/iDRAC-Benutzer zu konfigurieren.

   Im Fenster **Benutzerkonfiguration für Remote-Zugriff** können Sie einen bestimmten BMC/iDRAC-Benutzer konfigurieren.
4. Legen Sie folgende allgemeine Informationen fest:
   - Zur Aktivierung eines Benutzers wählen Sie **Benutzer aktivieren**.
   - Geben Sie einen Namen für den Benutzer in das Feld **Benutzername** ein.
   - Wählen Sie das Kontrollkästchen **Kennwort ändern** aus.
   - Geben Sie ein neues Kennwort in das Feld **Neues Kennwort** ein.
   - Geben Sie das gleiche Kennwort in das Bestätigungsfeld **Neues Kennwort bestätigen** ein.
5. Legen Sie folgende Benutzerberechtigungen fest:
   - Wählen Sie die maximalen Beschränkungen für LAN-Benutzerberechtigungsebenen aus.
   - Wählen Sie maximal gewährte serielle Schnittstellen-Benutzerberechtigung aus.
6. Geben Sie die Benutzergruppe für die DRAC/iDRAC-Benutzerberechtigungen an.
7. Klicken Sie auf **Änderungen anwenden**, um Änderungen zu speichern.
8. Klicken Sie auf **Zurück zum Fenster Remote-Zugriffsbenutzer**, um zum Fenster **Remote-Zugriffsbenutzer** zurückzukehren.



ANMERKUNG: Sechs zusätzliche Benutzereinträge sind konfigurierbar, wenn DRAC installiert ist. Dies ergibt insgesamt 16 Benutzer. Dieselben Benutzername- und Kennwortregeln gelten für BMC/iDRAC- und RAC-Benutzer. Wenn DRAC/iDRAC6 installiert ist, werden alle 16 Benutzereinträge DRAC zugewiesen.

Plattformereignisfilter-Warnungen einstellen

So konfigurieren Sie die wichtigsten BMC-Funktionen, darunter die Parameter für Plattformereignisfilter (PEF) und -Warnungsziele, über den Server Administrator-Instrumentierungsdienst:

1. Klicken Sie auf das Objekt **System**.
2. Klicken Sie auf das Register **Warnungsverwaltung**.
3. Klicken Sie auf **Plattformereignisse**.

   Über das Fenster **Plattformereignisse** können Sie einzelne Maßnahmen für bestimmte Plattformereignisse ergreifen. Sie können die Ereignisse auswählen, bei denen Sie Maßnahmen zum

Herunterfahren ergreifen wollen, und Warnungen für ausgewählte Maßnahmen generieren. Sie können auch Warnungen an bestimmte IP-Adressen Ihrer Wahl senden.

ANMERKUNG: Sie müssen mit Administratorberechtigungen angemeldet sein, um die BMC-PEF-Warnungen konfigurieren zu können.

ANMERKUNG: Mit der Einstellung **Plattformereignisfilter-Warnungen aktivieren** kann das Erzeugen von PEF-Warnungen deaktiviert oder aktiviert werden. Diese Einstellungen sind unabhängig von den einzelnen Plattformereignis-Warnungseinstellungen.

ANMERKUNG: **Systemstromsondenwarnungen** und **Systemstromsondenfehler** werden auf Dell PowerEdge-Systemen ohne PMBus-Unterstützung nicht unterstützt, obwohl Server Administrator die Konfiguration zulässt.

ANMERKUNG: Auf Dell PowerEdge 1900-Systemen werden die Plattformereignisfilter PS/VRM/D2D-Warnung, PS/VRM/D2D-Fehler und Netzteil nicht vorhanden nicht unterstützt, obwohl Server Administrator Ihnen erlaubt, diese Ereignisfilter zu konfigurieren.

4. Wählen Sie das Plattformereignis aus, für das Sie Maßnahmen zum Herunterfahren ergreifen wollen, oder generieren Sie Warnungen für ausgewählte Maßnahmen und klicken dann auf **Plattformereignisse festlegen**.

   Im Fenster **Plattformereignisse** festlegen können Sie Maßnahmen festlegen, die getroffen werden, wenn das System aufgrund eines Plattformereignisses heruntergefahren werden soll.

5. Wählen Sie eine der folgenden Maßnahmen:
   - **Keine**
   - **System neu starten**

     Fährt das Betriebssystem herunter und leitet einen Systemstart ein, wobei BIOS-Überprüfungen durchgeführt werden und das Betriebssystem neu geladen wird.
   - **System ausschalten**

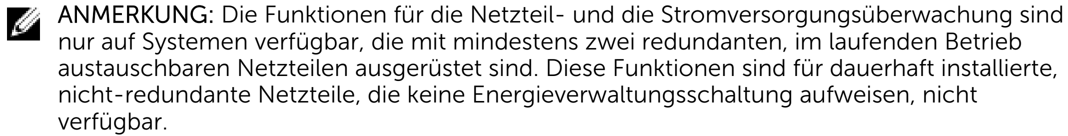
     Schaltet die Stromversorgung des Systems aus.
   - **System aus- und einschalten**

     Schaltet die Stromversorgung des Systems aus, pausiert, schaltet den Strom wieder ein und startet das System neu. Das Ein-und Ausschalten ist sinnvoll, wenn Sie Systemkomponenten wie Festplatten neu initialisieren möchten.
   - **Stromverminderung**

     Drosselt die CPU.



VORSICHT: Wenn Sie eine andere Plattformereignis-Maßnahme zum Herunterfahren als Keine oder Stromverminderung auswählen, wird Ihr System zwingend herunterfahren, wenn das angegebene Ereignis auftritt. Dieses Herunterfahren wird von der Firmware gestartet und ausgeführt, ohne das Betriebssystem oder irgendwelche Anwendungen herunterzufahren.



ANMERKUNG: Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

6. Markieren Sie das Kontrollkästchen **Warnung generieren**, um das Senden von Warnungen zu aktivieren.

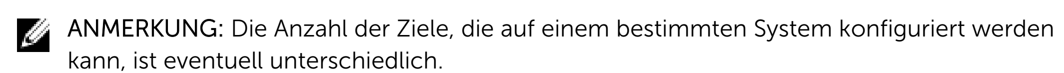
 ANMERKUNG: Zur Generierung einer Warnung muss sowohl die Einstellung **Warnung generieren** als auch die Einstellung **Plattformereigniswarnungen aktivieren** ausgewählt werden.

7. Klicken Sie auf **Anwenden**.
8. Klicken Sie auf **Anwenden zur Plattformereignisseite**, um zum Fenster **Plattformereignisfilter** zurückzukehren.

Plattformereigniswarnungsziele einstellen

Sie können auch über das Fenster Plattformereignisfilter ein Ziel auswählen, an das eine Warnung über ein Plattformereignis gesendet werden soll. Je nach Anzahl der Ziele, die auf Ihrem System angezeigt werden, können Sie eine separate IP-Adresse für jede Zieladresse konfigurieren. Eine Plattform Ereigniswarnungen wird an jede von Ihnen konfigurierte IP-Adresse gesendet.

1. Klicken Sie auf **Ziele konfigurieren** im Fenster Plattformereignisfilter.
2. Klicken Sie auf die Nummer des Zieles, das Sie konfigurieren möchten.



ANMERKUNG: Die Anzahl der Ziele, die auf einem bestimmten System konfiguriert werden kann, ist eventuell unterschiedlich.

3. Aktivieren Sie das Kontrollkästchen **Ziel aktivieren**.
4. Klicken Sie auf **Zielnummer**, um eine eigene IP-Adresse für dieses Ziel einzugeben. Diese IP-Adresse ist die IP-Adresse, an die die Plattformereigniswarnung gesendet wird.
5. Geben Sie einen Wert im Feld **Community-Zeichenkette** ein, der als Kennwort zur Authentifizierung von Meldungen zwischen einer Management Station und einem verwalteten System verwendet wird. Die Community-Zeichenkette (auch als Community-Name bezeichnet) wird in jedem Datenpaket zwischen Management Station und verwaltetem System gesendet.
6. Klicken Sie auf **Anwenden**.
7. Klicken Sie auf **Zurück zur Plattformereignisseite**, um zum Fenster **Plattformereignisfilter** zurückzukehren.

6

Server Administrator-Protokolle

Server Administrator ermöglicht die Anzeige und Verwaltung von Hardware-, Warnungs- und Befehlsprotokollen. Alle Benutzer können entweder von der Startseite von Server Administrator oder von dessen Befehlszeilenschnittstelle auf Protokolle zugreifen und Berichte drucken. Benutzer müssen mit Administrator-Berechtigungen angemeldet sein, um Protokolle zu löschen, oder sie müssen mit Admin- oder Hauptbenutzer-Berechtigungen angemeldet sein, um E-Mail-Protokolle an ihren festgelegten Dienstkontakt zu senden.

Informationen zum Anzeigen von Protokollen und zum Erstellen von Berichten über die Befehlszeile finden Sie im *Server Administrator Command Line Interface User's Guide* (Server Administrator Benutzerhandbuch zur Befehlszeilenoberfläche) unter **dell.com/openmanagemanuals**.

Beim Anzeigen der Server Administrator-Protokolle können Sie auf **Hilfe** klicken ( ), um detaillierte Informationen über das Fenster zu erhalten, das gerade zu sehen ist. Server Administrator-Protokollhilfe ist in allen Fenstern verfügbar, die dem Benutzer zugänglich sind, basierend auf den entsprechenden Zugriffsrechten und den spezifischen Hardware- und Softwaregruppen, die Server Administrator auf dem verwalteten System feststellt.

Integrierte Funktionen

Klicken Sie auf eine Spaltenüberschrift, um den Inhalt der Spalte zu sortieren oder die Sortierreihenfolge zu ändern. Außerdem enthält jedes Protokollfenster mehrere Task-Schaltflächen, die zur Verwaltung und Unterstützung des Systems verwendet werden können.

Protokollfenster-Task-Schaltflächen

Die folgende Tabelle führt die Protokollfenster-Task-Schaltflächen auf.

Tabelle 11. Protokollfenster-Task-Schaltflächen

Name	Beschreibung
Drucken	Um eine Kopie des Protokolls auf dem Standarddrucker zu drucken.
Exportieren	Um eine Textdatei mit den Protokolldaten (in der die Werte aller Datenfelder durch ein benutzerdefiniertes Begrenzungszeichen getrennt sind) an einem von Ihnen festgelegten Ort zu speichern.
E-Mail	Um eine E-Mail-Nachricht zu erstellen, die den Inhalt des Protokolls als Anhang einschließt.
Protokoll löschen	Um alle Ereignisse aus dem Protokoll zu löschen.

Name	Beschreibung
Speichern unter	Um den Protokollinhalt in einer **.zip**-Datei zu speichern.
Aktualisieren	Um den Protokollinhalt wieder in den Datenbereich des Maßnahmenfensters zu laden.



ANMERKUNG: Unter Task-Schaltflächen finden Sie weitere Informationen über die Task-Schaltflächen.

Server Administrator-Protokolle

Server Administrator enthält die folgenden Protokolle:

- Hardwareprotokoll
- Warnungsprotokoll
- Befehlsprotokoll

Hardwareprotokoll

Die Hardwareprotokoll-Statusanzeige ändert sich zum kritischen Status ( ) wenn die Protokolldatei 100 Prozent der Kapazität erreicht. Es gibt zwei verfügbare Hardwareprotokolle, abhängig vom System: das ESM-Protokoll (Embedded System Management-Protokoll) und das SEL-Protokoll (Systemereignisprotokoll). Das ESM- und das SEL-Protokoll bestehen jeweils aus einem Satz integrierter Anweisungen, die Hardwarestatusmeldungen an Systemverwaltungssoftware senden können. Jede in den Protokollen verzeichnete Komponente hat ein Statusanzeigensymbol neben der Bezeichnung. Die folgende Tabelle listet die Statusanzeigen.

Tabelle 12. Hardwareprotokoll-Statusanzeigen

Status	Beschreibung
Ein grünes Kontrollhäkchen ( )	zeigt an, dass eine Komponente in Ordnung (normal) ist.
Ein gelbes Dreieck mit einem Ausrufezeichen ( )	zeigt an, dass für eine Komponente ein Warnzustand (nicht kritisch) besteht, der sofortige Aufmerksamkeit erfordert.
Ein rotes X ( )	zeigt eine kritische Bedingung (Ausfall) für eine Komponente an, die eine Aufmerksamkeit erfordert.
Ein Fragezeichen-Symbol ( )	gibt an, dass der Funktionszustand der Komponente nicht bekannt ist.

Zum Zugriff auf das Hardware-Protokoll klicken Sie auf **System**, dann auf das Register **Protokolle** und auf **Hardware**.

In den ESM- und SEL-Protokollen enthaltene Informationen umfassen:

- Den Schweregrad des Ereignisses
- Das Datum und die Uhrzeit, zu der das Ereignis erfasst wurde

- Eine Beschreibung des Ereignisses

Unterhalt des Hardwareprotokolls

Das Statusanzeigesymbol neben dem Protokollnamen auf der Server Administator-Startseite wechselt vom normalen Status ( ) zum nicht-kritischen Status ( ), wenn die Protokolldatei 80 Prozent der Kapazität erreicht. Stellen Sie sicher, dass Sie das Hardwareprotokoll löschen, wenn 80 Prozent der Kapazität erreicht sind. Wenn dem Protokoll erlaubt wird, 100 Prozent der Kapazität zu erreichen, werden die neuesten Ereignisse aus dem Protokoll entfernt und verworfen.

Klicken Sie zum Löschen eines Hardware-Protokolls auf der Seite **Hardware-Protokoll** auf die Verknüpfung **Protokoll löschen**.

Warnungsprotokoll



ANMERKUNG: Falls das Warnungsprotokoll ungültige XML-Daten anzeigt (wenn zum Beispiel die für die Auswahl generierten XML-Daten nicht angemessen formatiert sind), klicken Sie auf **Protokoll löschen** und zeigen Sie die Protokolldaten noch einmal an.

Mit dem Warnungsprotokoll können verschiedene Systemereignisse überwacht werden.Server Administrator erzeugt Ereignisse als Reaktion auf Änderungen im Status von Sensoren und anderen überwachten Parametern. Jedes Statusänderungsereignis, das im Warnungsprotokoll aufgezeichnet wird, besteht aus einem eindeutigen Bezeichner, genannt Ereignis-ID, für die spezifische Ereigniskategorie und einer Ereignismeldung, die das Ereignis beschreibt. Ereignis-ID und -Meldung beschreiben den Schweregrad und die Ursache des Ereignisses eindeutig und enthalten weitere relevante Informationen wie z. B. die Stelle des Ereignisses und den vorherigen Status der überwachten Komponente.

Zum Zugriff auf das Warnungsprotokoll klicken Sie auf **System**, dann auf das Register **Protokolle** und auf **Warnung**.

Im Warnungsprotokoll enthaltene Informationen umfassen:

- Den Schweregrad des Ereignisses
- Die Ereignis-ID
- Das Datum und die Uhrzeit, zu der das Ereignis erfasst wurde
- Die Kategorie des Ereignisses
- Eine Beschreibung des Ereignisses



ANMERKUNG: Der Protokollverlauf wird später u. U. zur Behebung von Fehlern oder für Diagnosezwecke benötigt. Es wird deshalb empfohlen, die Protokolldateien zu speichern.



ANMERKUNG: OMSA kann ggf. duplizierte SNMP-Traps oder duplizierte Ereignisse auf der Warnungsprotokoll-Seite oder in der Betriebssystem-Protokolldatei protokollieren. Die duplizierten Traps und Ereignisse werden protokolliert, wenn die OMSA-Dienste manuell neu gestartet werden, oder wenn der Gerätesensor einen nicht der Norm entsprechenden Zustand angibt, wenn die OMSA-Dienste nach dem Neustarten eines Betriebssystems gestartet werden.

Detaillierte Informationen zu Warnmeldungen finden Sie im *Server Administrator Messages Reference Guide* (Server Administrator-Meldungs-Referenzhandbuch) unter **dell.com/openmanagemanuals**.

Befehlsprotokoll



ANMERKUNG: Falls das Befehlsprotokoll ungültige XML-Daten anzeigt (wenn zum Beispiel die für die Auswahl generierten XML-Daten nicht angemessen formatiert sind), klicken Sie auf **Protokoll löschen** und zeigen Sie die Protokolldaten noch einmal an.

Verwenden Sie das Befehlsprotokoll zur Überwachung aller vom Server Administrator ausgegebenen Befehle. Das Befehlsprotokoll verzeichnet An- und Abmeldungen, Systemverwaltungssoftware-Initialisierungen und ein von der Systemverwaltungssoftware eingeleitetes Herunterfahren und protokolliert den Zeitpunkt, an dem das Protokoll zuletzt gelöscht wurde. Die Größe der Befehlsprotokolldatei kann gemäß Ihrer Anforderung angegeben werden.

Zum Zugriff auf das Befehlsprotokoll klicken Sie auf **System**, dann auf das Register **Protokolle** und auf **Befehl**.

Im Befehlsprotokoll enthaltene Informationen umfassen:

- Das Datum und die Uhrzeit, zu der der Befehl gegeben wurde
- Der Benutzer, der derzeit auf der Server Administrator-Startseite oder der CLI angemeldet ist
- Eine Beschreibung des Befehls und der zugehörigen Werte



ANMERKUNG: Der Protokollverlauf wird später u. U. zur Behebung von Fehlern oder für Diagnosezwecke benötigt. Es wird deshalb empfohlen, die Protokolldateien zu speichern.

7

Warnungsmaßnahmen einstellen

Warnungsmaßnahmen einstellen für Systeme, auf denen unterstützte Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssysteme ausgeführt werden

Wenn Sie Warnungsmaßnahmen für ein Ereignis einstellen, können Sie die Maßnahme Warnung auf dem Server anzeigen festlegen. Um diese Maßnahme auszuführen, sendet Server Administrator eine Meldung an /dev/console. Wenn auf dem Server Administrator-System ein X Window System ausgeführt wird, wird diese Meldung nicht angezeigt. Um die Warnungsmeldung auf einem Red Hat Enterprise Linux-System zu sehen, wenn X Window System ausgeführt wird, müssen Sie **xconsole** oder **xterm -C** starten, bevor das Ereignis eintritt. Um die Warnungsmeldung auf einem SUSE Linux Enterprise Server-System zu sehen, wenn X Window System ausgeführt wird, müssen Sie ein Terminal wie **xterm -C** starten, bevor das Ereignis eintritt.

Beim Einstellen von Warnungsmaßnahmen für ein Ereignis können Sie die **Rundsendung einer Meldung** als Aktion festlegen. Zum Ausführen dieser Aktion führt Server Administrator den Befehl wall aus, mit dem die Meldungen an jeden gesendet wird, der angemeldet ist und dessen Nachrichtenberechtigung auf **Ja** gesetzt ist. Wird auf dem Server Administrator-System ein X Window-System ausgeführt, können Sie diese Meldung standardmäßig nicht sehen. Zum Anzeigen der Meldung, während das X Window-System ausgeführt wird, müssen Sie ein Terminal wie **xterm** oder **gnome-terminal** starten, bevor das Ereignis eintritt.

Wenn Warnungsmaßnahmen für ein Ereignis eingestellt werden, kann die Maßnahme für **Anwendungsprogramm ausführen** angegeben werden. Für die Anwendungen, die Server Administrator ausführen kann, gelten Einschränkungen. Um eine ordnungsgemäße Ausführung zu gewährleisten:

- Geben Sie keine X Windows-System-basierten Anwendungen an, da Server Administrator solche Anwendungen nicht ordnungsgemäß ausführen kann.
- Geben Sie keine Anwendungen an, bei denen Eingaben durch den Benutzer erforderlich sind, da Server Administrator solche Anwendungen nicht richtig ausführen kann.
- Leiten Sie **stdout** und **stderr** beim Festlegen der Anwendung in eine Datei um, sodass Ausgaben oder Fehlermeldungen angezeigt werden.
- Wenn mehrere Anwendungen (oder Befehle) für eine Warnung ausgeführt werden sollen, erstellen Sie ein Skript, das diese Aufgabe übernimmt, und geben Sie den vollständigen Pfad zum Skript in das Feld **Absoluter Pfad zur Anwendung** ein.

Beispiel 1: `ps -ef >/tmp/psout.txt 2>&1`

Der Befehl in Beispiel 1 führt die Anwendung ps aus, leitet stdout in die Datei **/tmp/psout.txt** um und leitet **stderr** in dieselbe Datei wie **stdout** um.

Beispiel 2: `mail -s "Serverwarnung" admin /tmp/mailout.txt 2>&1`

Der Befehl in Beispiel 2 führt die Mail-Anwendung aus, um die Meldung in der Datei /tmp/alertmsg.txt mit dem Betreff **Serverwarnung** an den Red Hat Enterprise Linux-Benutzer oder SUSE LINUX Enterprise

Server-Benutzer und Administrator zu senden. Die Datei **/tmp/alertmsg.txt** muss vom Benutzer erstellt werden, bevor das Ereignis eintritt. **stdout** und **stderr** können außerdem in die Datei **/tmp/mailout.txt** umgeleitet werden, falls ein Fehler eintritt

Einstellen von Warnungsmaßnahmen in Microsoft Windows Server 2008

Bei der Angabe von Warnungsmaßnahmen werden Visual Basic-Skripts nicht automatisch von der Funktion "Anwendung ausführen" interpretiert, obwohl Sie die Dateien `.cmd, .com, .bat,, .exe` ausführen können, indem nur die Datei als die Warnungsmaßnahme angegeben wird.

Rufen Sie zur Lösung dieses Problems zuerst den Befehlsprozessor `cmd.exe` auf, um Ihr Script zu starten. So kann beispielsweise die Behandlungsmaßnahmen zum Ausführen einer Anwendung wie folgt eingestellt werden:

```
c:\winnt\system32\cmd.exe /c d:\example\example1.vbs
```

wobei `d:\example\example1.vbs` der vollständige Pfad zur Script-Datei ist.

Legen Sie im Feld „Absoluter Pfad zur Anwendung" keinen Pfad zu einer interaktiven Anwendung (eine Anwendung mit grafischer Benutzeroberfläche oder eine Anwendung, die Benutzereingaben erfordert) fest. Unter bestimmten Betriebssystemen funktionieren interaktive Anwendungen möglicherweise nicht einwandfrei.



ANMERKUNG: Sie müssen den vollständig Pfad sowohl für **cmd.exe** als auch die Skriptdateien angeben.

Warnungsmaßnahme zum Ausführen einer Anwendung in Windows Server 2008 einstellen

Aus Sicherheitsgründen ist Windows Server 2008 so konfiguriert, dass interaktive Dienste nicht zulässig sind. Ist ein Dienst in Windows Server 2008 als interaktiver Dienst installiert, protokolliert das Betriebssystem eine Fehlermeldung an das Windows Systemprotokoll, der gemäß dieser Dienst als interaktiver Dienst markiert wird.

Wenn Sie Server Administrator zum Konfigurieren von Warnungsmaßnahmen für ein Ereignis verwenden, können Sie das Ausführen einer Anwendung als Aktion festlegen. Damit interaktive Anwendungen für eine Warnungsmaßnahme ordnungsgemäß ausgeführt werden, muss der Dell Systems Management Server Administrator (DSM SA)-Datenverwaltungsservice als interaktiver Dienst konfiguriert sein. Beispiele interaktiver Anwendungen sind Anwendungen mit grafischer Benutzeroberfläche (Graphical User Interface, GUI) oder Anwendungen, die den Benutzer zu einer Eingabe auffordern, wie z.B. der Befehl pause in einer Stapeldatei.

Wenn Server Administrator auf einem Microsoft Windows Server 2008 installiert ist, so ist der DSM SA-Datenverwaltungsservice als nicht-interaktiver Dienst installiert, d.h. er ist standardmäßig so konfiguriert, dass er nicht mit dem Desktop interagieren kann. Daher werden interaktive Anwendungen im Rahmen einer Warnungsmaßnahme nicht ordnungsgemäß ausgeführt. Wenn in diesem Falle eine interaktive Anwendung als Warnungsmaßnahme ausgeführt wird, pausiert die Anwendung und wartet auf Eingabe. Die Benutzerschnittstelle bzw. Eingabeaufforderung der Anwendung ist für Sie jedoch nicht sichtbar und

bleibt auch dann nicht sichtbar, wenn der Dienst zur Erkennung interaktiver Dienste gestartet wird. Das **Ablaufregister** im Task-Manager zeigt einen Anwendungsablauf-Eintrag für jede Ausführung der interaktiven Anwendung an.

Wenn Sie eine interaktive Anwendung für eine Warnungsmaßnahme auf Microsoft Windows Server 2008 ausführen müssen, müssen Sie den DSM SA-Datenverwaltungsservice so konfigurieren, dass er mit dem Desktop interagieren und interaktive Dienst aktivieren kann.

So erlauben Sie die Interaktion mit dem Desktop:

- Klicken Sie mit der rechten Maustaste auf den DSM SA-Datenverwaltungsservice im Fenster **Dienste**steuerung, und wählen Sie **Eigenschaften** aus.
- Aktivieren Sie auf der Registerkarte **Anmelden** die Option **Interagieren von Service zu Desktop erlauben**, und klicken Sie auf **OK**.
- Starten Sie DSM SA-Datenverwaltungsservice neu, damit die Änderung wirksam wird.
- Stellen Sie sicher, dass der Dienst zur **Ermittlung interaktiver Dienste** ausgeführt wird.

Wenn der DSM SA-Datenverwaltungsservice mit dieser Änderung neu gestartet wird, generiert der Manager für die Dienstesteuerung die folgende Fehlermeldung im Systemprotokoll:

```
Der DSM SA-DSM SA-Datenverwaltungsservice wird als interaktiver Dienst
gekennzeichnet. Durch die Aktivierung des Dienstes zur Ermittlung von
interaktiven Diensten kann der DSM SA-Datenverwaltungsservice interaktive
Anwendungen für eine Warnungsmaßnahme ordnungsgemäß ausführen.
```

Sobald diese Änderungen durchgeführt sind, wird das Dialogfeld **Interaktive Dienste-Dialogerkennung** durch das Betriebssystem angezeigt, um Zugriff auf die interaktive Anwendungsschnittstelle/ Eingabeaufforderung zu ermöglichen.

Warnungsmeldungen der BMC/iDRAC-Plattformereignisfilter

In der folgenden Tabelle werden alle möglichen Meldungen für Plattformereignisfilter mit einer Beschreibung des entsprechenden Ereignisses angezeigt.

Tabelle 13. PEF-Warnungsereignisse

Ereignis	Beschreibung
Lüftersonden-Fehler	Der Lüfter läuft zu langsam oder überhaupt nicht.
Spannungssondenfehler	Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus.
Batteriesondenwarnung	Die Batterie wird unterhalb der empfohlenen Aufladungsstufe betrieben.
Batteriesondenfehler	Die Batterie ist ausgefallen.
Diskreter Spannungssondenfehler	Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus.
Temperatursondenwarnung	Der Temperaturwert nähert sich einer Hoch- oder Niedriggrenze.
Temperatursonden-Fehler	Der Temperaturwert ist für einen ordnungsgemäßen Betrieb entweder zu hoch oder zu niedrig.
Gehäuseeingriff festgestellt	Das Systemgehäuse wurde geöffnet.

Ereignis	Beschreibung
Redundanz (Netzteil oder Lüfter) herabgesetzt	Die Redundanz der Lüfter bzw. Netzteile wurde herabgesetzt.
Redundanz (Netzteil oder Lüfter) verloren	Es besteht keine Redundanz mehr für die Lüfter und/oder Netzteile des Gehäuses.
Prozessorwarnung	Ein Prozessor läuft unter seiner Spitzenleistung bzw. Taktrate.
Prozessorfehler	Ein Prozessor ist ausgefallen.
Prozessor nicht vorhanden	Ein Prozessor wurde entfernt.
PS/VRM/D2D-Warnung	Das Netzteil, das Spannungsreglermodul oder der DC/DC-Konverter steht vor einem Ausfall.
PS/VRM/D2D-Fehler	Netzteil, Spannungsreglermodul oder DC/DC-Konverter ist fehlerhaft.
Hardwareprotokoll ist voll oder wurde geleert	Ein leeres oder volles Hardwareprotokoll erfordert die Aufmerksamkeit des Administrators.
Automatische Systemwiederherstellung	Das System hängt bzw. reagiert nicht, und es werden von der automatischen Systemwiederherstellung konfigurierte Maßnahmen getroffen.
Systemstromsondenwarnung	Die Leistungsaufnahme nähert sich dem Fehlerschwellenwert.
Systemstromsondenfehler	Die Leistungsaufnahme hat die höchstzulässige Stufe überschritten, was zu einem Fehler führte.
Wechselbarer Flash-Datenträger nicht vorhanden	Der wechselbare Flash-Datenträger wurde entfernt.
Fehler bei wechselbarem Flash-Datenträger	Für den wechselbaren Flash-Datenträger steht ein Fehlerzustand an.
Wechselbarer Flash-Datenträger – Warnung	Für den wechselbaren Flash-Datenträger steht ein Fehlerzustand an.
Kritisch für interne zweifache SD-Modulkarte	Die interne zweifache SD-Modulkarte ist ausgefallen.
Warnung für interne zweifache SD-Modulkarte	Für die interne zweifache SD-Modulkarte steht ein Fehlerzustand an.
Redundanzverlust für interne zweifache SD-Modulkarte	Die interne zweifache SD-Modulkarte verfügt nicht über Redundanz.
Interne zweifache SD-Modulkarte nicht vorhanden	Die interne zweifache SD-Modulkarte wurde entfernt.

8

Fehlerbehebung

Verbindungsdienstfehler

Auf Red Hat Enterprise Linux startet der D\SM-SA-Verbindungsdienst (Dell Systems Management Server Administrator) nicht, wenn `SELinux is set to enforced mode`. Führen Sie einen der folgenden Schritte aus, und starten Sie diesen Dienst:

- Stellen Sie `SELinux` auf den Modus `Disabled` oder den Modus `Permissive` ein.
- Ändern Sie die SELinux-Eigenschaft **allow_execstack** zum Zustand **EIN**. Führen Sie den folgenden Befehl aus:

  ```
  setsebool allow_execstack on
  ```

- Ändern Sie den Sicherheitskontext für den SM-SA-Verbindungsdienst. Führen Sie den folgenden Befehl aus: `chcon -t unconfined_execmem_t /opt/dell/srvadmin/sbin/dsm_om_connsvcd`

Anmeldefehler-Szenarien

Eine Anmeldung beim Managed System kann in folgenden Situationen fehlschlagen:

- Eingabe einer ungültigen/falschen IP-Adresse.
- Eingabe falscher Anmeldeinformationen (Benutzername und Kennwort).
- Das Managed System ist AUSgeschaltet.
- Das Managed System ist aufgrund einer ungültigen IP-Adresse oder eines DNS-Fehlers nicht erreichbar.
- Das Managed System weist ein nicht vertrauenswürdiges Zertifikat auf und Sie wählen auf der Anmeldeseite nicht **Zertifikatswarnung ignorieren** aus.
- Die Server Administrator-Dienste sind auf dem VMware ESXi-System nicht aktiviert. Im *Server Administrator Installation Guide* (Installationshandbuch zu Server Administrator) unter **dell.com/openmanagemanuals** finden Sie Informationen darüber, wie Server Administrator-Dienste auf dem VMware ESXi-System aktiviert werden.
- Der SFCBD-Dienst (small footprint CIM broker daemon) des VMware ESXi-Systems wird nicht ausgeführt.
- Der Web Server-Verwaltungsdienst auf dem verwalteten System wird nicht ausgeführt.
- Wenn Sie das Kontrollkästchen **Zertifikatswarnung ignorieren** nicht aktivieren, geben Sie die IP-Adresse des verwalteten Systems und nicht den Host-Namen ein.
- Die WinRM-Berechtigungsfunktion (Remoteaktivierung) ist auf dem verwalteten System nicht konfiguriert. Informationen zu dieser Funktion finden Sie im *Server Administrator Installation Guide* (Server Administrator-Installationshandbuch) unter **dell.com/openmanagemanuals**.
- Beim Versuch, eine Verbindung zu einem VMware ESXi 5.0-Betriebssystem herzustellen, tritt ein Authentifizierungsfehler auf, was sich möglicherweise auf einen der folgenden Gründe zurückführen lässt:

a. Der Sperrmodus `lockdown` ist aktiviert, während Sie beim Server oder bei Server Administrator angemeldet sind. Weitere Informationen zum Sperrmodus `lockdown` finden Sie in der VMware-Dokumentation.
b. Das Kennwort wird geändert, während Sie bei Server Administrator angemeldet sind.
c. Sie melden sich bei Server Administrator als normaler Benutzer ohne Administratorrechte an. Weitere Informationen zum Zuweisen der Rolle finden Sie in der VMware-Dokumentation.

Beheben einer fehlerhaften Server Administrator-Installation auf einem unterstützten Windows-Betriebssystem

Sie können eine fehlerhafte Installation beheben, indem Sie eine Neuinstallation erzwingen und anschließend Server Administrator deinstallieren.

So erzwingen Sie eine Neuinstallation:

1. Prüfen Sie, welche Version von Server Administrator zuvor installiert war.
2. Laden Sie das Installationspaket für diese Version unter **support.dell.com** herunter.
3. Machen Sie SysMgmt.msi im Verzeichnis srvadmin\windows\SystemsManagement ausfindig.
4. An der Befehlseingabeaufforderung geben Sie den folgenden Befehl ein, um eine Neuinstallation zu erzwingen

```
msiexec /i SysMgmt.msi REINSTALL=ALL

REINSTALLMODE=vamus
```

5. Wählen Sie **Benutzerdefiniertes Setup** aus, und wählen Sie alle Funktionen aus, die ursprünglich installiert wurden. Wenn Sie nicht sicher sind, welche Funktionen installiert wurden, wählen Sie alle Funktionen aus und führen Sie die Installation aus.

   ANMERKUNG: Wenn Sie Server Administrator in einem Standardverzeichnis installiert haben, stellen Sie sicher, dass die Änderung auch in **Benutzerdefiniertes Setup** durchgeführt wird.

   ANMERKUNG: Sobald die Anwendung installiert ist, können Sie Server Administrator unter Verwendung von **Programme hinzufügen/entfernen** deinstallieren.

Server Administrator-Dienste

Die folgende Tabelle führt die von Server Administrator verwendeten Dienste zur Bereitstellung von Systemverwaltungsinformationen sowie die Folgen eines Ausfalls dieser Dienste auf.

Tabelle 14. Server Administrator-Dienste

Dienstname	Beschreibung	Fehlerwirkung	Wiederherstellungsmechanismus	Schweregrad
Windows: SM-SA-Verbindungsdienst Linux: `dsm_om_connsvc` (Dieser Dienst wird mit dem Server Administrator Web Server installiert.)	Bietet Remote-/lokalen Zugriff auf Server Administrator von beliebigen Systemen mit einem unterstützten Webbrowser und	Benutzer können sich nicht bei Server Administrator anmelden, und keine Vorgänge über die Web-Benutzeroberfläche ausführen. CLI	Dienst neu starten	Kritisch

Dienstname	Beschreibung	Fehlerwirkung	Wiederherstellung smechanismus	Schweregrad
	einer unterstützten Netzwerkverbindung aus.	kann jedoch nach wie vor verwendet werden.		
Windows: SM SA-Freigabedienste Linux: `dsm_om_shrsvc` (Dieser Dienst wird auf dem Managed System ausgeführt.)	Legt beim Start eine Bestandsaufnahme der Systemsoftware an, über die SNMP- und CIM-Anbieter von Server Administrator eine Remote-Softwareaktualisierung mithilfe der Dell System Management Console und des Dell IT Assistant (ITA) durchführen.	Softwareaktualisierungen sind unter Verwendung des ITA nicht möglich. Jedoch können die Aktualisierungen lokal und außerhalb von Server Administrator mithilfe einzelner Dell Update-Pakete durchgeführt werden. Aktualisierungen können weiterhin über Drittanbieter-Tools (darunter MSSMS, Altiris und Novell ZENworks) vollzogen werden.	Dienst neu starten	Warnung

 ANMERKUNG: OMSA kann ggf. duplizierte SNMP-Traps oder duplizierte Ereignisse auf der Warnungsprotokoll-Seite oder in der Betriebssystem-Protokolldatei protokollieren. Die duplizierten Traps und Ereignisse werden protokolliert, wenn die OMSA-Dienste manuell neu gestartet werden, oder wenn der Gerätesensor einen nicht der Norm entsprechenden Zustand angibt, wenn die OMSA-Dienste nach dem Neustarten eines Betriebssystems gestartet werden.

 ANMERKUNG: Der Bestandsaufnahmensammler muss Dell Konsolen unter Verwendung von Dell Update Packages aktualisieren.

 ANMERKUNG: Einige Funktionen des Bestandsaufnahmensammlers werden von OMSA (64–Bit) nicht unterstützt.

Dienstname	Beschreibung	Fehlerwirkung	Wiederherstellung smechanismus	Schweregrad
Windows: SM SA-Datenmanager Linux: `dsm_sa_datamgrd` (im Dienst dataeng gehostet) (Dieser Dienst wird auf dem Managed System ausgeführt.)	Überwacht das System, bietet schnellen Zugriff auf detaillierte Fehler- und Leistungsinformationen und erlaubt Remoteverwaltung überwachter Systeme, einschließlich Herunterfahren, Start und Sicherheit.	Wenn diese Dienste nicht ausgeführt werden, sind Benutzer nicht in der Lage, die Details der Hardware-Ebene auf der GUI/CLI zu konfigurieren/ anzuzeigen.	Dienst neu starten	Kritisch
Windows: DSM SA-Ereignismanager	Bietet einen Dienst zur	Wenn dieser Dienst angehalten wird,	Dienst neu starten	Warnung

Dienstname	Beschreibung	Fehlerwirkung	Wiederherstellungsmechanismus	Schweregrad
Linux: `dsm_sa_eventmgrd` (im Dienst dataeng gehostet) (Dieser Dienst wird auf dem Managed System ausgeführt.)	Ereignisprotokollierung von Betriebssystemen und Dateien für die Systemverwaltung und wird auch von Ereignisprotokollanalysatoren verwendet.	werden die Funktionen der Ereignisprotokollierung nicht einwandfrei funktionieren.		
Linux: `dsm_sa_snmpd` (im Dienst dataeng gehostet) (Dieser Dienst wird auf dem Managed System ausgeführt.)	Data Engine-SNMP-Schnittstellte von Linux	SNMP Get/Set/Trap-Anforderung funktioniert nicht über eine Management Station.	Dienst neu starten	Kritisch
Windows: `mr2kserv` (Dieser Dienst wird auf dem Managed System ausgeführt.)	Der Speicherverwaltungsdienst gibt Auskunft über die Speicherverwaltung und erweiterte Funktionen zur Konfiguration eines lokalen oder entfernten Speichers, der mit einem System verbunden ist.	Benutzer sind nicht in der Lage, Speicherfunktionen für alle unterstützten RAID- und Nicht-RAID-Controller auszuführen.	Dienst neu starten	Kritisch

9

Häufig gestellte Fragen

In diesem Abschnitt werden die häufig gestellten Fragen zu Server Administrator aufgelistet:

ANMERKUNG: Die folgenden Fragen beziehen sich nicht ausschließlich auf die vorliegende Version von Server Administrator.

1. **Warum tritt ein Fehler bei der ESXi 5.x Host-Neustartfunktion vom Server Administrator auf?**

   Dieses Problem taucht auf Grund des VMware Stand-Alone License (SAL)-Schlüssels auf. Weitere Informationen finden Sie im Knowledge Base-Artikel unter **kb.vmware.com/kb/kb1026060**.

2. **Welche Berechtigungsebene muss ein Benutzer mindestens haben, um Server Administrator zu installieren?**

   Um Server Administrator zu installieren, müssen Sie über Administratorrechte verfügen. Hauptbenutzer und reguläre Benutzer haben keine Berechtigung, Server Administrator zu installieren.

3. **Ist ein Upgrade-Pfad erforderlich, um Server Administrator zu installieren?**

   Führen Sie bei Systemen mit Server Administrator in Version 4.3 eine Aktualisierung auf eine 6.*x*-Version und anschließend auf eine 7.*x*-Version durch. Führen Sie bei Systemen mit einer Version unterhalb von Version 4.3 zunächst eine Aktualisierung auf Version 4.3, dann auf eine 6.*x*-Version und dann auf eine 7.*x*-Version durch. (Das *x* steht hier für die Version von Server Administrator, auf die Sie aktualisieren möchten).

4. **Wie kann ich feststellen, welches die aktuellste Version von Server Administrator ist, die für mein System erhältlich ist?**

   Melden Sie sich an bei: **dell.com/support** → Software & Sicherheit → Enterprise System Management → OpenManage Server Administrator.

   Alle verfügbaren Versionen von Server Administrator werden auf der Seite angezeigt.

5. **Wie kann ich feststellen, welche Version von Server Administrator auf meinem System ausgeführt wird?**

   Nachdem Sie sich am Server Administrator angemeldet haben, wechseln Sie zu **Eigenschaften** → **Zusammenfassung**. Die auf Ihrem System installierte Version von Server Administrator wird in der Spalte **Systemverwaltung** angezeigt.

6. **Gibt es noch andere Schnittstellen außer 1311, die Benutzer verwenden können?**

   Ja, Sie können Ihre bevorzugte https-Schnittstelle einstellen. Wechseln Sie zu **Einstellungen →Allgemeine Einstellungen→Web Server→HTTPS-Schnittstelle**

   Wählen Sie statt **Standardeinstellung verwenden** die Option Optionsschaltfläche **verwenden**, um Ihre bevorzugte Schnittstelle festzulegen.

   ANMERKUNG: Die Änderung der Anschlussnummer auf eine ungültige bzw. eine bereits belegte Anschlussnummer kann andere Anwendungen oder Browser beim Zugriff auf den Server Administrator auf dem verwalteten System behindern. Eine Liste der Standardschnittstellen finden Sie im Dell OpenManage *Server Administrator-Installationshandbuch* unter dell.com/openmanagemanuals.

7. **Kann ich Server Administrator auf Fedora, College Linux, Mint, Ubuntu, Sabayon oder PClinux installieren?**

Nein, Server Administrator unterstützt keines dieser Betriebssysteme.

8. **Kann Server Administrator beim Auftreten eines Problems E-Mails senden?**

   Nein, Server Administrator ist nicht dafür ausgelegt, bei Problemen E-Mails zu senden.

9. **Ist SNMP für die ITA-Ermittlung, die Bestandsaufnahme und Softwareaktualisierungen auf PowerEdge-Systemen erforderlich? Kann CIM für Ermittlung, Bestandsaufnahme und Aktualisierungen alleine verwendet werden oder ist SNMP erforderlich?**

   ITA-*Kommunikation mit Linux-Systemen*:

   SNMP ist auf dem Linux-System für Ermittlung, Statusabfrage und Bestandsaufnahme erforderlich.

   Softwareaktualisierungen werden über eine SSH-Sitzung und sicheres FTP vorgenommen. Für diese diskrete Maßnahme sind Berechtigungen/Anmeldeinformationen auf Stammebene erforderlich, die dann eingegeben werden müssen, wenn die Maßnahme eingerichtet bzw. angefordert wird. Anmeldeinformationen des Ermittlungsbereichs werden nicht vorausgesetzt.

   ITA-*Kommunikation mit Windows-Systemen*:

   Für Server (Systeme, die Windows Server-Betriebssysteme ausführen) kann das System entweder mit SNMP oder mit CIM oder mit beiden Protokollen zur Ermittlung durch ITA konfiguriert werden. Bestandsaufnahme erfordert CIM.

   Softwareaktualisierungen, wie bei Linux, stehen nicht mit Ermittlung, Abfrage und den verwendeten Protokollen in Verbindung.

   Unter Verwendung der Anmeldeinformationen auf Administratorebene, die zum Zeitpunkt der Aktualisierungsplanung oder -ausführung angefordert werden, wird eine administrative (Laufwerk-) Freigabe auf ein Laufwerk des Zielsystems eingerichtet, und Dateien werden von einem Speicherort (möglicherweise eine andere Netzwerkfreigabe) auf das Zielsystem kopiert. Daraufhin werden WMI-Funktionen aufgerufen, um die Softwareaktualisierung auszuführen.

   Auf Clients/Workstations wird Server Administrator nicht installiert. Die CIM-Ermittlung wird daher verwendet, wenn das Zielsystem die OpenManage Client Instrumentation ausführt.

   Für viele andere Geräte, wie z. B. Netzwerkdrucker, kommuniziert SNMP weiterhin standardmäßig mit dem (in erster Linie ermittelten) Gerät.

   Geräte wie EMC-Speicher haben proprietäre Protokolle. Bestimmte Informationen zu dieser Umgebung können über die Schnittstellen gesammelt werden.

10. **Gibt es Pläne für SNMP-v3-Unterstützung?**

    Nein, es gibt keine Pläne für SNMP v3-Unterstützung.

11. **Verursacht ein Unterstreichungszeichen im Domänennamen Probleme bei der Anmeldung bei Server Admin?**

    Ja, ein Unterstreichungszeichen im Domänennamen ist ungültig. Auch alle anderen Sonderzeichen (außer dem Bindestrich) sind ungültig. Es sind ausschließlich Buchstaben, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, sowie Zahlen zu verwenden.

12. **Welchen Einfluss hat das Markieren/Aufheben der Markierung von 'Active Directory' auf der Anmeldungsseite von Server Administrator auf Berechtigungsebenen?**

    Wenn Sie das Kontrollkästchen "Active Directory" nicht markieren, haben Sie nur den Zugriff, der im Microsoft Active Directory konfiguriert ist. Sie können sich nicht unter Verwendung der erweiterten Schemalösung von bei Microsoft Active Directory anmelden.

Diese Lösung ermöglicht Ihnen, Zugriff auf Server Administrator zu gewähren. Sie können damit Server Administrator-Benutzer und -Berechtigungen zu bestehenden Benutzern in Ihrer Active Directory-Software hinzufügen bzw. steuern. Weitere Informationen finden Sie unter "Microsoft Active Directory verwenden" im *Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) unter **dell.com/openmanagemanuals**.

13. **Welche Maßnahmen muss ich treffen, während ich eine Kerberos-Authentifizierung ausführe und eine Anmeldung über den Web Server versuche?**

    Für Authentifizierungen müssen die Inhalte der Dateien **/etc/pam.d/openwsman** und **/etc/pam.d/sfcb** auf dem verwalteten Knoten durch Folgendes ersetzt werden:

    Für 32-Bit:

    ```
    auth required pam_stack.so service=system-auth auth required /lib/security/
    pam_nologin.so account required pam_stack.so service=system-auth
    ```

    Für 64-Bit:

    ```
    auth required pam_stack.so service=system-auth auth required /lib64/
    security/pam_nologin.so account required pam_stack.so service=system-auth
    ```

14. **Warum ist das Betriebssystem von Red Hat Enterprise Linux 5.9 (32-Bit) nicht in der Lage, die Emulex-Karte nach der Installation der Emulex-Treiber zu erkennen?**

    Auf Systemen, die Red Hat Enterprise Linux 5.9 (32-Bit)-Betriebssysteme ausführen, ist der Emulex-Treiber abhängig von den folgenden RPMs:

    - kernel-headers-2.6.18-346,el5,i386,rpm
    - glibc-headers-2,5-107,i386,rpm
    - glibc-devel-2,5-107,i386,rpm
    - gcc-4.1.2-54,el5,i386,rpm

    Wenn eins der oben aufgeführten RPMs fehlt, hat das System Probleme bei der Erkennung der Emulex Netzwerkadapter.